jamk.fi

Cloud outsourcing guidelines and data protection regulation in Europe

Context of online banking self-service channels

Tomi Pulkkinen

Master's thesis
April 2018
School of Technology, Communication and Transport
Information Technology
Degree Programme in Cyber Security

Jyväskylän ammattikorkeakoulu
JAMK University of Applied Sciences

jamk.fi

Description

Author(s)	Type of publication	Date
Pulkkinen, Tomi	Master's thesis	April 2018
		Language of publication: English
	Number of pages: 90	Permission for web publication: x

Title of publication

Cloud outsourcing guidelines and data protection regulation in Europe

Context of online banking self-service channels

Degree programme

Cyber Security

Supervisor(s)

Rantonen, Mika

Huotari, Jouni

Assigned by

Tieto Finland Oy

Abstract

The objective of the master's thesis was to describe a compliance service architecture for self-service channels in online banking conforming to the EU General Data Protection Regulation and European Banking Authority's (EBA) recommendations on outsourcing to cloud. Research methods were based on legal dogmatics and qualitative deduction.

During 2017, EBA published a draft recommendations on outsourcing to cloud for undertakings. At the time of research, neither EBA's recommendation nor EU General Data Protection Regulation were yet effective, which meant results and conclusions are based on interpretations and comparisons to existing legislation and guidelines rather than based on judgements or decisions made by authorities in respect to renewed recommendations and regulation.

As a result, a number of design principles, security controls, privacy techniques, functional, non-functional, contractual and process level requirements were identified as part of the compliance service architecture. The requirements were classified against the control objectives and controls of ISO-IEC 27001 and ENISA Information Assurance Framework.

It was also concluded, that the regulative landscape of outsourcing to cloud is permissive; however, there are specific requirements such as audit and access requirements spanning to the whole outsourcing chain, which can be challenging to meet contractually.

A risk-based approach in conjunction with formal, systematic approach in classifying and implementing requirements, securing contractual rights and defining service performance indicators for measuring contract performance are the backbone of a successful outsourcing arrangement and basis of compliance architecture.

Keywords/tags (subjects)

Online banking, outsourcing, compliance, cloud security

jamk.fi

Kuvailulehti

Tekijä(t)	Julkaisun laji	Päivämäärä
Pulkkinen, Tomi	Opinnäytetyö, ylempi AMK	Huhtikuu 2018
	Sivumäärä 90	Julkaisun kieli Englanti
		Verkkojulkaisulupa myönnetty: x

Työn nimi

Cloud outsourcing guidelines and data protection regulation in Europe

Context of online banking self-service channels

Tutkinto-ohjelma

Cyber Security

Työn ohjaaja(t)

Rantonen, Mika

Huotari, Jouni

Toimeksiantaja(t)

Tieto Finland Oy

Tiivistelmä

Opinnäytetyössä tavoitteena oli kuvata vaatimustenmukainen arkkitehtuuri Euroopan pankkiviranomaisen (EBA) pilveen ulkoistamisen suositusten ja EU:n tietosuoja-asetuksen (EU GDPR) pohjalta.

Vuoden 2017 aikana Euroopan pankkiviranomainen (EBA) valmisteli luonnoksen suosituksista valvottaville ulkoistamisesta pilvipalveluntarjoajille. Suositus ja uusi EU-tasoinen henkilötieto-asetus (EU GDPR) eivät olleet vielä voimassa opinnäytetyöprosessin aikana. Tulokset pohjautuvat tulkintoihin suositusten ja lainsäädännön pohjalta. Tutkimusmenetelminä hyödynnettiin lainoppia ja laadullista päättelyä luokittelun pohjalta.

Tuloksena tunnistettiin ja kerättiin joukko suunnitteluperiaatteita, tietoturvakontrolleja, yksityisyydensuojan tekniikoita, toiminnallisia ja ei-toiminnallisia sekä sopimuksellisia että prosessitason vaatimuksia. Vaatimukset luokiteltiin ISO-IEC 27001:2013 standardin ja ENISA:n Information Assurance –kehyksen pohjalta.

Lisäksi suositusten pohjalta todettiin, että sääntely on itsepalvelukanavien näkökulmasta sallivaa, mutta esimerkiksi sopimuksellinen auditointi- ja pääsyoikeuksien turvaaminen koko pilvipalveluntarjoajan ulkoistusketjussa on haastavaa.

Riskienhallintaan pohjautuva systemaattinen, kirjallinen vaatimusten luokittelu ja implementointi, sopimuksellisten vaatimusten turvaaminen ja palvelutason mittareiden määrittely valvonnan mahdollistamiseksi, ovat onnistuneen ulkoistuksen ja vaatimustenmukaisen arkkitehtuurin peruspilareita.

Avainsanat (asiasanat)

Verkkopankki, ulkoistaminen, vaatimustenmukaisuus, pilvipalvelut, tietoturva

Muut tiedot

Contents

Figures

Tables

1 Introduction

The regulatory climate in European banking sector has been in turbulence since 2008 financial crisis, that started in the subprime mortgage market in the United States, and then expanded into global scale. The crisis meant increased burden of capital requirements, new requirements with regards to corporate governance arrangements and processes and financial reporting for the banks (A comprehensive EU response to the financial crisis 2014, Introduction). In 2018, there are several new regulations, which Financial Institutions need to have implemented such as Network and Information Security Directive, EU General Data Protection Regulation and Payment Services Directive 2, the two latter requiring most of the effort to comply with.

In May 2017, European Banking Authority started the process of drafting recommendations for outsourcing to cloud computing, built on the existing Guidelines on outsourcing developed by the Committee of European Banking Supervisors (CEBS) in 2006 but extending its scope further to address the use of cloud computing. The intent is to clarify the EU-wide supervisory expectations if Financial Institutions intend to adopt cloud computing, so as to allow them to leverage the benefits of using cloud services, while ensuring that any related risks are adequately identified and managed (Recommendations on outsourcing to cloud service providers 2017).

Based on replies to European Commission Consultation on FinTech, both Finnish (Finanssivalvonta 2017a, 12) and Swedish (Finansinspektionen's response to the Commission Consultation Document on FinTech 2017, 1) Financial Supervisory Authorities have a positive and constructive attitude towards outsourcing to cloud; however, they emphasize meeting financial sector specific regulations such as right to perform inspections through contractual arrangements. Finansinspektionen's administrative fine of 25 million SEK to Nasdaq Clearing Aktiebolag in 2016 demonstrates that outsourcing monitoring and risk management can be a challenging task for a financial institution (Decision FI Ref 15-9258, 2016). According to European Union Agency for Network and Information Security (ENISA) publication Secure Use of Cloud Computing in the Finance Sector, cloud computing is gradually

being adopted within the European financial industry while the vast majority of financial institutions still rely on in-house infrastructure. The report further reveals, that the approach for cloud adoption is not yet mature and it is being adopted to only a limited number of use cases. (Secure Use of Cloud Computing in the Finance Sector 2015, 5).

PSD2 regulation requires banks to grant third party access for Payment Service Providers or Account Information Service Providers without extra costs to their customers' accounts and payment services securely following customer consent. PSD2 regulation and Open Banking Initiatives yet extending the PSD scope shape the competition landscape, which forces Financial Institutions to adapt to changes more rapidly and reposition themselves in the digital value chain. European Banking Federation members share a view that digitalization is one of the main methods for banks to increase their competitiveness, with 90% of banks stating that digitalization is a priority for them. The growth of FinTech and digital payment solutions provide particularly interesting opportunities. (Competitiveness of European Banks and Financial Technology 2017.)

This master's thesis focuses on conforming to EU General Data Protection Regulation and outsourcing guidelines of European Supervisory Authority in the context of outsourced, cloud based self-service channels in online banking. Prior research work available focuses on:

- customers' perspectives on adoption of cloud computing in finance sector (Cloud Computing - Factors that affect an adoption of cloud computing in traditional Swedish banks by Emma Lundberg and Caroline Åkesson, 2015),
- data protection in cloud computing in Sweden (Data protection in cloud computing – The Swedish perspective by Dan Svantesson, 2012),
- and developing a reference architecture for financial services in the cloud (Banking 2.0: Developing a Reference Architecture for Financial Services in The Cloud by Ana Bucur, 2011). However, none of these theseis focus on summarizing and linking compliance requirements in financial sector to an architectural and regulatory context.

There is no commonly recognized definition for online banking self-service channels, which means some effort is spent on explaining and defining the boundaries of the context and service architecture and finally interpreting what this means from the compliance point of view. Overall, a self-service channel could consist of capabilities and artifacts such as contracts, IT processes and business continuity, technical

architecture and capabilities, (requirements on) skills and knowledge for operating the service context. By channels, one could understand mobile bank, Internet bank, Interactive voice response (IVR) technology, corporate banking clients or any 3rd party applications delivered over PSD2 APIs, where the APIs would be the channel to the infrastucture of a Financial Institution. Ana Bucur's thesis (2011, 74) coins out a definition of Customer Interaction Cloud as a solution package or component being part of a banking reference architecture taking care of all customer interaction integrating mobile accessibility, Internet portal and Call Center solution. The scope of Customer Interaction Cloud and Front Office Distribution Channels of the thesis corresponds on a high-level to the scope of this master's thesis; however, this thesis does not take any product-centric approach in blueprinting the solution components nor is it based on any proprietary architectural models to come up with a reference architecture.

The motivation behind this thesis is to create a reference of applying relevant financial industry recommendations and regulations to a business and technical context. As context, financial self-service channels are in the focal point of digitalization, customer engagement and experience, new PSD2 enabled business models, online threats, fraud and in addition subject of rapid cycle of innovation.

2 Research strategy

2.1 Thesis structure

In the approach to the research presented here, the thesis begins with formulation of the research problem and context, followed by a description of qualitative research methods, data collection and data analysis.

The research context is introduced in more detail with the definitions of solution architecture, operative environment and identification of relevant and applicable compliance schemes. These are also one of the starting activities in the approach outlined by ISO 19600 compliance management system based on the continual improvement Plan-Do-Check-Act principle as illustrated in (Figure 1). (ISO/IEC 19600:2014, Introduction).

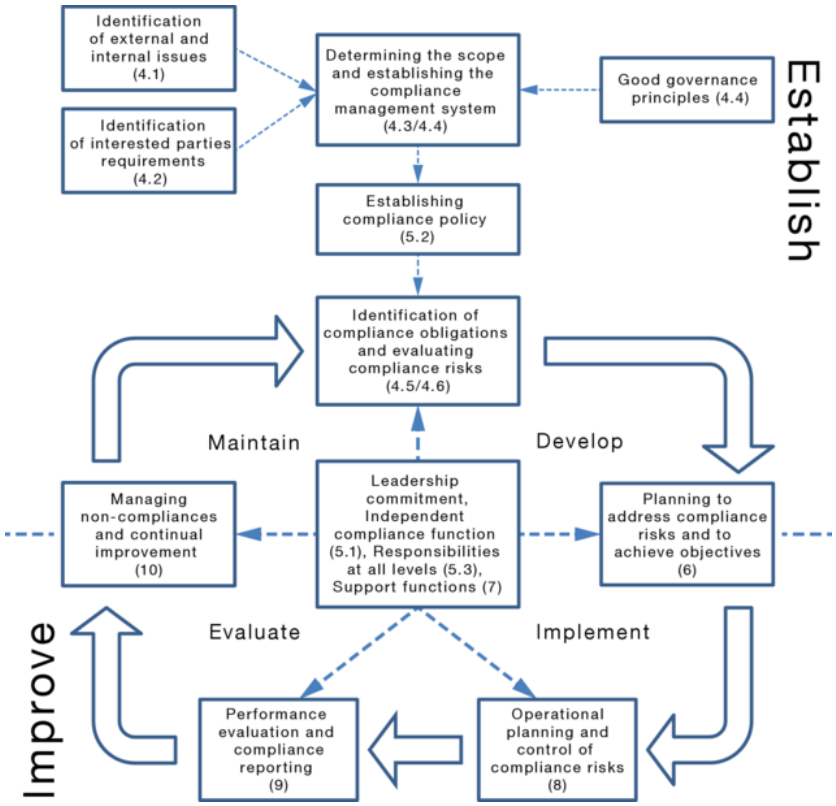

Figure 1. Flowchart of ISO 19600 compliance management system

After identification of the external and internal issues and the requirements of the interested parties, ISO 19600 proposes to determine the scope and establish the compliance management system (Compliance management systems — Guidelines 2014).

The research context is followed by a deep-dive into each of the regulations, guidelines, recommendations and interpretations within the scope of cloud outsourcing and data protection as well as summarization and classification of the topic in hand to form a requirement base.

The requirement base is used to reverse engineer an abstract compliance solution architecture for online banking self-service channels, which link the architecture and requirements together.

Conclusions and suggestions on future research around the research problems are described in the end of the thesis.

2.2 Research field

Legal informatics is interdisciplinary and strives to complement the traditional legal perspective with perspectives from the field of informatics (Seipel 2010, 32). As a science, it researches the relationship between law and information, law and information technology, and issues arising from regulation and interpretations of the regulation in the operating environment. More specifically this thesis falls into the category of information technology law (IT law). Information technology law refers to the legal field that examines legal regulation and interpretation issues relating in particular to the design, implementation and use of IT solutions including IT-based products and services. (Saarenpää 1998, 1.)

2.3 Research problem

There is plenty of research and publications on e.g. outsourcing, data protection regulation or cloud security in general, however there are less sources focusing on a specific business service, domain and technological context. Without a well-defined context-setting, an outsourcing institution and a service provider are both more likely to cause misunderstanding and struggle in fulfilling their obligations and share of legal and information security risks.

Key research questions of the thesis are wrapped around following themes:

- What regulations, guidelines, recommendations and proprietary standards apply to outsourcing of online banking self-service channels?
- How does the scope of business requirements or technical architectural boundaries affect the number of regulatory provisions?
- What characteristics does a compliant architecture have and what aspects does it consists of?
- What type of compliance issues related to outsourcing do the financial institutions struggle?
- What type of compliance issues do service providers struggle with in financial services domain?
- What is the supervisory attitude or climate on outsourcing in general and outsourcing to cloud?
- How a standard compliance management system help an undertaking to mitigate compliance risks

2.4 Research objectives

The objective of this thesis is to provide a comprehensive view on legal frameworks, recommendations and requirements applicable to online banking channels such as mobile and Internet bank in an outsourced delivery environment. The compliance requirements are further translated into a compliance solution architecture in the given context based on interpretations of the compliance requirements. The thesis further attempts to interpret potential pitfalls in complying with the regulations and recommendations.

The application of the thesis work can help a service provider to reduce mutual commercial risks by providing information what type of security controls, processes and reporting is required on a practical level and guide towards a compliant service contract. It can also help by giving a baseline of risks for risk analysis and risk management process. From the financial institution point of view, added value could be found in common vocabulary and gaining understanding for discussing the requirements and their practical mitigation strategies with a service provider and capability to recognize characteristics, which a compliant architecture should have.

2.5 Research methods

As the thesis consists of both interpretations of law and compliance requirements but also blueprinting a compliance architecture, its research methods utilize legal dogmatics and are based on qualitative deduction. Legal dogmatics is associated with interpretations and systematization of legal norms (Aarnio 1999, 334).

Abstraction and blueprinting of solution architecture based on requirements is a result of both textual data analysis, interpretation of the regulations and deduction of conclusions made on how those requirements can be met. Deduction is generally drawn and concluded from established facts and evidence (Leavy 2014, 588).

2.6 Data collection

Qualitative data sources in general include observation, fieldwork, interviews, questionnaires, documents, texts and the researcher's impressions and reactions of

the researcher (Whitman & Woszczynski 2004, 309). In this thesis qualitative data sources are based on publicly available resources such as regulations, consultation papers, surveys and technical guidelines (RTS) of European Banking Authority, annual reports and rulings or decisions of Financial Supervisory Authorities and earlier research work in the financial services domain in Europe.

2.7 Data analysis

Data analysis is based on qualitative content analysis. Ole Holsti (1969, 14) offers a broad definition of content analysis as any technique for making inferences by objectively and systematically identifying specified characteristics of messages. Klaus Krippendorff (2013, 24) has stated that "Content analysis is a research technique for making replicable and valid inferences from data in their context".

The requirement base of data collection is analyzed by coding and categorizing against ISO 27001:2013 and ENISA Cloud Computing Information Assurance Framework. The key sections of ENISA Cloud Computing Information Assurance Framework framework are based on the broad classes of information security controls from the ISO 27001/2 and BS25999 standards (Information Assurance Framework 2009, Methodology). Any indirect evidence in form of an obligation is recursively abstracted back to a recommendation or a requirement.

The objectives and controls of ISO 27001:2013 were seen as most suitable framework compared to 27032:2012 and ENISA Cloud Computing Information Assurance Framework correlating well with the requirements set by EBA for outsourcing. ENISA IAF emphasizes more data portability, which is abstracted to business continuity and exit strategies by EBA outsourcing regulation. According to Segovia (ISO 27001 & ISO 22301, 2015), controls that can be found in ISO 27032:2012 are more specific for cybersecurity such as application level controls, server protection, end-user and social engineering attack controls. In comparison ISO 27001:2013 standard of information security management is more generic, less concrete, extensive and global without cyber security emphasis.

2.8 Reliability of data collection and analysis

As the renewed outsourcing recommendation to cloud by European Banking Authority is not yet well established, there are no case examples of supervisory assessments based on the recommendation. However some of the decisions or rulings can be interpreted as applicable also under the new recommendation as only minor refactoring is done in considering the unique characteristics of cloud computing and cloud based services. Some of the same old concerns still remain with the new recommendations and legislation entering into force. This will have some impact on the reliability of interpretations due to the lack of official interpretations by authorities or court. Instead, the interpretations are as good as the quality of the different sources, showing interest in interpreting the data protection regulation and contributing to outsourcing recommendations, and that they are used as references in this thesis work.

Due the fact that security and non-compliance are sensitive topics in financial industry, which is largely based on consumer and market trust, not all information is publicly published by Financial Supervisory Authorities supervising the financial institutions. This is evident when comparing the difference between volume and the level of material published by Finnish and Swedish Financial Supervisory Authorities. There is more public auditing information published by Finansinspektionen. Therefore, the identified best practices or demonstration of compliance as means of evidence to be produced to meet a specific recommendation or guideline is by no means inclusive.

Lastly, using systematically defined coding protocols improves measurement by removing elements of researcher biases and improving thoroughness and accuracy. However, content analysis as a method loses relevance and ability to reach important aspects of legal interpretation in cases, where coding objectively is almost impossible due to nuances related to infrequent or highly complex factual and procedural patterns. (Hall 2011, 6).

3 Compliance management systems for establishing context and compliance risk management

Adoption of a compliance management system is a good practice to demonstrate regulators and authorities that an organization is seeking to be in line with the regulative provisions or guidelines. ISO 19600 also follows a risk-based approach in which the identified risks in context of compliance requirements and commitments are the basis of action. (Ernst & Young LLP, 2015). EU General Data Protection Regulation sets a requirement, where the controller should be obliged to implement appropriate and effective measures and be able to demonstrate the compliance of processing activities with this Regulation, including the effectiveness of the measures (European Parliament and the Council of the European Union 2016, 14).

ISO 19600 guidelines on compliance management systems are applicable to all types of organizations, but the extent of the application of the guidelines depends on the size, structure, nature and complexity of the organization (Compliance management systems - Guidelines 2014).

By looking at the structure of the standard reflected on e.g. Figure 1, it can be seen that there is an emphasis on structuring and aligning the organization with the effort required to have a holistic view on compliance. Work packages such as good governance principles, identification of interested parties, leadership and commitment, independent compliance function, responsibilities at all levels, are all examples of continuous support and commitment for compliance work in order to come up with a culture, which produces behavioral norms conducive to compliance outcomes.

This thesis does not focus on describing a case study on how to organize compliance management. Instead, the same risk-based approach was applied to identify compliance risks in thesis context in Chapter 12. Identification of compliance risks was a one-off effort and at this stage, as it was sufficient to only have a list of risks instead of planning, what is their priority or exact mitigation plan.

However, what is worth analyzing, is the root cause of non-conformance or noncompliance. Nonconformance occurs when something does not meet the

specifications or requirements in some way. Noncompliance is the failure to adhere to an Act or its Regulations. Examples of root causes could be lack of competent resourcing, lack of independent compliance function or lead role, not considering compliance as integral part of “definition of done” of business service development or lack of practice of measuring and reporting compliance. Analysis and continuous improvement are parts of performance evaluation and compliance reporting as well as managing non-compliances and continual improvement as suggested by ISO 19600:2014 standard.

4 Regulatory and outsourcing context of the thesis

The outsourcing context of this thesis is limited to outsourcing instructions of guidelines published by European Banking Authority for national supervisory authorities of the EU member states. The same applies to EU General Data Protection Regulation.

Most EU member states have comprehensively transposed the CEBS guidelines, the current guiding framework regulating outsourcing activities. A survey carried out by the EBA during 2015 indicated, that of the 24 national frameworks 53% totally transposed, 38% partially transposed and 8% did not transpose the CEBS guidelines. (European Banking Authority 2017a, 21). Due the fact that the thesis has been written before access to information to which extent the recommendations on outsourcing to cloud will be transposed in different EU member states, the thesis focuses on understanding the baseline, that national supervisory authorities are expected to implement under the ‘comply or explain’ principle.

Some references are also made to statements of Finnish and Swedish national supervisory authorities, which are in specific interests of the company behind the thesis assignment.

There are two primary factors having impact on the outsourcing context: the category of financial institution e.g. a credit institution or investment firm impacting applicable outsourcing guidelines and regulations and secondly the architectural boundaries of the business domain related to outsourced online banking channels.

The architectural boundaries are explained further in the chapter on compliance architecture.

The outsourcing context of the thesis focuses on both IT Outsourcing (ITO) as well as Application Development and Maintenance (ADM), where the former has been a very traditional and active area of outsourcing as illustrated below in Figure 2 and having focuses less on Business Process (BPO) or Knowledge Process Outsourcing (KPO). Offering online banking channel as an outsourced service means at least combination of both ITO and ADM types of outsourcing based on Software as a Service delivery model.

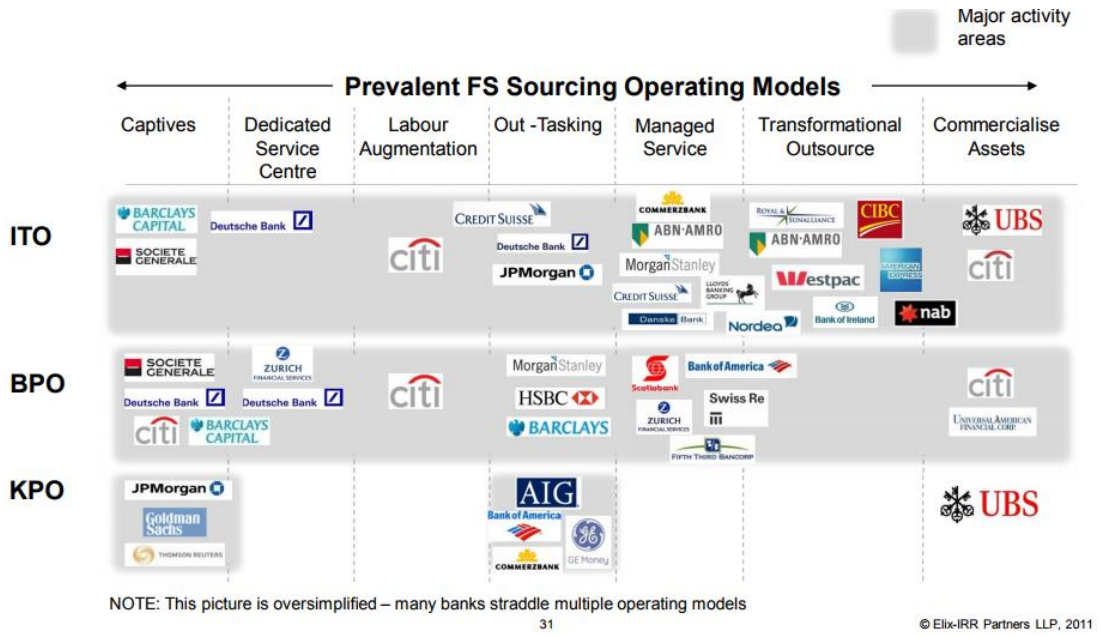

Figure 2: References of FS Sourcing Operating Models in 2010 (Elix-IRR Partners, 2011).

Because online banking channels stand for branding, customer engagement, customer experience and end customer business process innovation, which are all challenging to measure as KPIs, financial institutions want to maintain control and ownership over how their channels are further developed according to their business

strategy. Therefore outsourcing online banking channels is not about pure Business Process Outsourcing, which according to Gartner's definition means the delegation of one or more IT-intensive business processes to an external provider that, in turn, owns, administrates and manages the selected processes based on defined and measurable performance metrics (Gartner, 2018). However, the outsourcing context of the thesis does cover processes such as IT administration, service monitoring, service support and further development (implementation) of the services according to specifications of financial institutions.

Examples of Knowledge Process Outsourcing are banking and financial research services, market research, analytics, auditing and legal services, which could be perceived as add-on outsourcing services part of a service portfolio.

5 Regulative climate on outsourcing to cloud in Finland and Sweden

5.1 Finanssivalvonta (FIN-FSA)

Finanssivalvonta's response to FinTech survey by European Banking Authority (EBA) concluded that the recommendations of EBA together with generic security and privacy regulations provide a sufficient basis for regulating cloud computing services (Public consultation on FinTech 2017, 12). Further in the response (ibid., 12.), Finanssivalvonta states it does not see any specific regulatory or supervisory obstacles, that would prevent financial services firms from using cloud computing services as long as both the financial sector specific and generic regulations, such as general data protection, online privacy and NIS, are met. Finanssivalvonta does highlight in the response (ibid., 12.) the fact that financial institution must ensure that the national competent authorities' rights to perform inspections are guaranteed through contractual arrangements made with the cloud computing service.

5.2 Finansinspektionen (SWE-FSA)

Based on a response by Finansinspektionen to FinTech survey carried out by European Banking Authority (EBA), the financial supervisory authority of Sweden recognizes within banking industry the interest in cloud services and it being a driver for innovation; however also the challenges due uncertainty of supervisory expectations (Finansinspektionen's response to the Commission Consultation Document on FinTech 2017, 4). In the same response (ibid., 4.) Finansinspektionen announces taking a positive stance on upcoming EBA recommendations on outsourcing to cloud service providers. According to Finansinspektionen (ibid., 4.) the recommendation provides the clarity needed for adopting cloud computing and ensures that risks are appropriately identified and managed.

The latest statement titled "Promemoria" from Finansinspektionen (2018, 1) concluded, that even if in some cases cloud services contribute for more stable IT environments and ultimately better and cheaper financial services for consumers, the services also involve risks that need to be addressed. A company that wants to use cloud services must ensure that the company, its auditors and FI have access to relevant information and suitable premises if necessary to be able to check and on-site inspect the outsourced business at a cloud service provider (ibid., 1).

If a cloud service provider for legitimate reasons wants to restrict access to e.g. a datacenter, and an unlimited access is not necessary to check the outsourced operations, the need for such limitation according to Finansinspektionen (SWE-FSA) does not necessarily prevent the company from entering into an agreement. However, agreements with restrictions for auditing must have been through thorough risk analysis. They also need to be able to convince Finansinspektionen (SWE-FSA), why the restrictions do not affect the company's control capabilities. (ibid., 1).

6 Overview and structure of Financial Supervision and regulation in Europe

6.1 Supervising authorities

The European Banking Authority (EBA) is one of the specialized EU agencies set up by the European Parliament and the Council of the European Union. In accordance with Article 16 of Regulation (EU) No 1093/2010 (“the EBA regulation”), EBA issues guidelines and recommendations addressed to competent authorities, with a view to establish consistent, efficient and effective supervisory practices and ensure the common, uniform and consistent application of European Union law (EBA 2017a, 5).

Each EU member country has a local, national supervisory authority, for example Finanssivalvonta, the Financial Supervisory Authority (FIN-FSA), is the authority for supervision of Finland’s financial and insurance sectors established and authorized in Act on the Financial Supervisory Authority (Finanssivalvonta 2017b, Supervisory Disclosure).

The illustration in Figure 3 covers the regulative bodies and key documents in the context of the thesis. The data protection regulation is directly applicable to each of the European countries starting from 25 May 2018.

The deadline for competent authorities to report whether they comply with the cloud outsourcing recommendations will be two months after the publication of the translations, which were not yet available at the time of writing. The recommendations will apply from 1 July 2018. (ibid., 4). In the meanwhile, the national outsourcing guidelines continue to be effective until they are revised. The recommendations are not exhaustive, and should be read in conjunction with the CEBS guidelines (ibid., 7).

Payment Service Directive 2 has a sub-RTS defining requirements for Strong Authentication in respect to acting as Payment Initiation Service Providers (PISP) or Account Information Service Providers (AISP), which sets requirements for online banking customer strong authentication process for making payments.

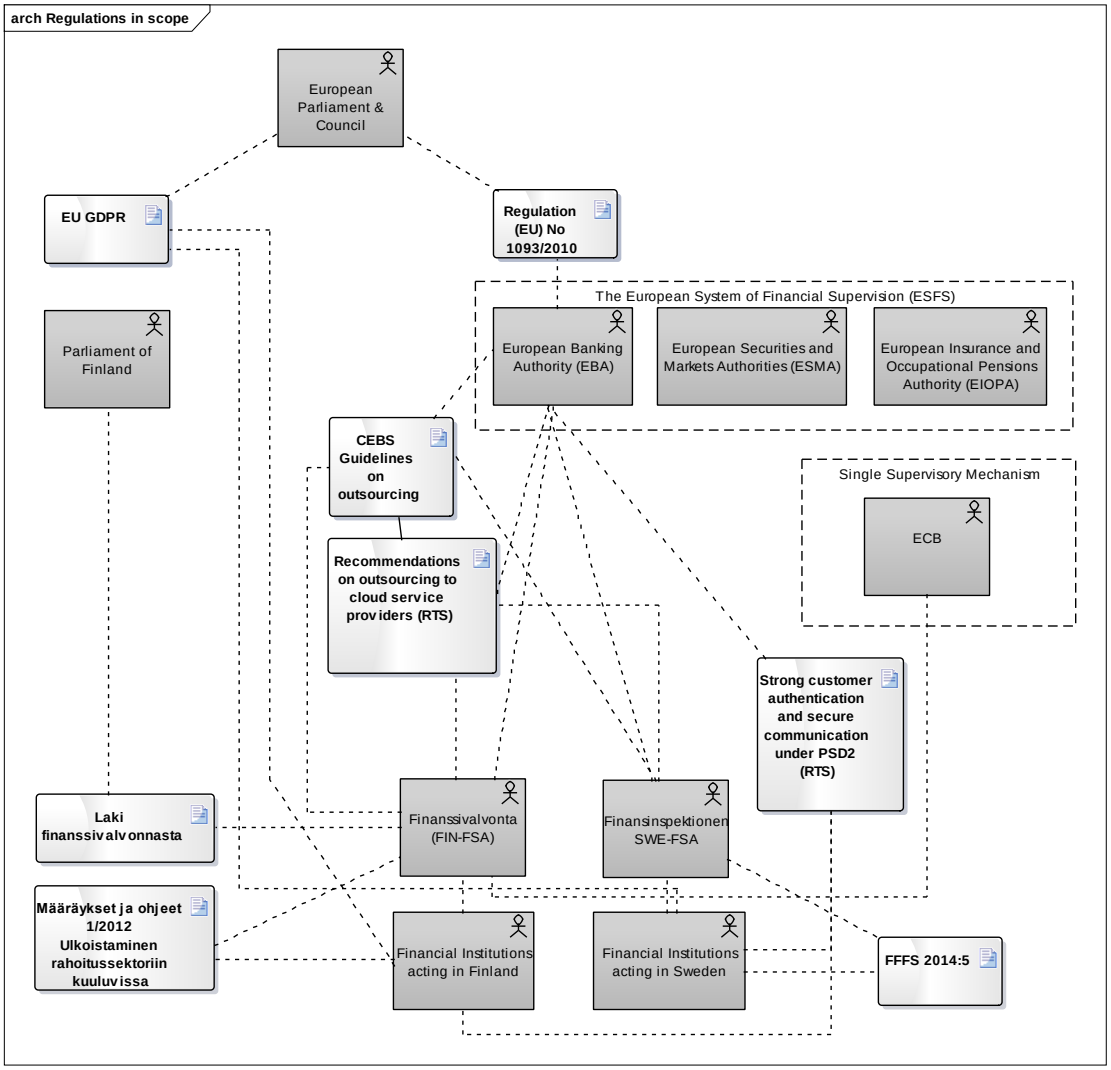

Figure 3: key regulative bodies, authorities and regulations illustrated in thesis context

6.2 Relevant regulation in context of online banking self-service channels

During the writing of the master's thesis, three regulations and guidelines were identified to have major impact on the content of the thesis: EU GDPR, CEBS Guidelines on Outsourcing and Recommendations on Cloud Outsourcing of European Banking Authority, where the latter is built on top of principles set in CEBS guidelines and should be read in conjunction with CEBS. In addition there are other regulations, which could be applicable to online banking channel's business or system architecture, which do not introduce additional requirements to outsourcing context

as such as PCI-DSS, Payment Service Directive 2, European Anti-Money Laundering and Countering the Financing of Terrorism (AML/CFT), electronic identification and trust services for electronic transactions in the internal market. In addition, EBA Guidelines on ICT risk under the Supervisory Review and Evaluation process introduces several control assessment requirements for authorities, which in reverse can be interpreted as implementation requirements. These requirements are aimed for financial institutions to e.g. secure websites and applications that can be directly attacked from the internet or the outside, and that can serve as an entry point into the internal ICT systems in a specific way (European Banking Authority 2017b, 28).

7 Analysis on interpretations of regulations and guidelines based on sanctions and decisions of National Financial Supervisory Authorities

There is a significant difference in terms of publicity and sanctions between the approach Finanssivalvonta (FIN-FSA) and Finansinspektionen (SWE-FSA) have steered financial institutions on outsourcing.

7.1 Finanssivalvonta (FIN-FSA)

According to Finanssivalvonta's (2013) presentation slides, they have done audits on operative risk management e.g. in the area of retail and corporate Internet banking services, IT outsourcing and especially continuity planning in system renewal projects. Further, Finanssivalvonta's (2015) annual report from year 2015 states it has carried out auditing on security of Internet banking, IT risk management, IT outsourcing, continuity planning and preparedness for incidents.

According to the same presentation (ibid), supervised entities including financial institutions, pension and insurance companies the continuity planning should be more accurate, do not always provide sufficient guiding and should be tested more often. In addition, information is typically not backed up to a third location outside dual site setup. (Finanssivalvonta, 2013).

There were no public remarks or sanctions in the area of outsourcing or operative risk management given by Finanssivalvonta nor any generalized report available for the public. Instead the room of improvement has been handled according to the process one-to-one between the supervisory authority and a financial institution and some hints on activities and generalized improvement areas can be found in e.g. presentations.

The only information available about the findings is the list available on the presentation highlighting challenges in operative risk management including strengthening of the risk assessment function, providing instructions with better quality for different areas (e.g. operative risk management, continuity planning, AML, KYC), risk reporting and transparency to board of directors, more accurate process descriptions and risk assessments, more efficient follow-up of IT programs, backup and continuity arrangements for payment transactions, training for Anti-Money Laundering (AML) and Know Your Customer (KYC). (Finanssivalvonta, 2013).

To summarize these findings per category of control are illustrated in Table 1 below. As a conclusion, none of the findings are related to challenges in outsourcing or data protection as such.

Table 1: Samples of operative risks identified during assessments by Finanssivalvonta (FIN-FSA)

Finding	Category
Strengthening of the risk assessment function	7 Support, 7.1 Resources
Instructions with better quality for different areas	8 Operation 8.1 Operational planning and control
Risk reporting and transparency to board of directors	6.1.2 Information security risk assessment
More efficient follow-up of IT programs	A.6.1.5 Information security in project management

Backup and continuity arrangements for payment transactions	A.17.2.1 Availability of information processing facilities

7.2 Finansinspektionen (SWE-FSA) and case Nasdaq Clearing

In 2016, Finansinspektionen focused on assessing how companies managed cyber risks (Finansinspektionen 2016b, 1). In case of Nasdaq Clearing, the company holds authorization to provide clearing services as a central counterparty. Finansinspektionen conducted the same investigation at their sister company, Nasdaq Stockholm Aktiebolag, which operates the regulated market, Nasdaq Stockholm. The Nordic subsidiaries in the Nasdaq Group, including Nasdaq Clearing, have outsourced a large part of their functions to the parent company, Nasdaq Inc. including, among others, information security. (ibid., 2).

Finansinspektionen found issues in the areas of outsourcing, risk management and business continuity. Regardless of the fact that the gaps were identified against provisions set out in Regulation (EU) No 648/2012 of the European Parliament and of the Council of 4 July 2012 on OTC derivatives, central counterparties and trade repositories (EMIR), the gaps are perfect examples of the risks European Banking Authority wants to avoid by publishing recommendations for credit institutions and investment firms. This case example pinpoints all the key pitfalls in the outsourcing domain.

The outsourcing contract s contained no detailed descriptions of the current services, quality measures (KPIs) nor did it have a formal service level agreement (SLA) (ibid., 5).

The company had no evidence to show, that they have received continuous information or follow-up statistics that provide an overview of the service delivery nor there was ongoing follow-up of the agreement and the delivery. Since the agreement has lacked SLA for information security services, in practice it was not possible for the company to carry out any detailed monitoring. Finansinspektionen's

opinion is that effective monitoring of outsourced functions requires in minimum a regular follow-up of the delivery. (Finansinspektionen 2016b, 6).

According to Finansinspektionen's evaluation, Nasdaq Clearing, as regards to cyber security, had in practice delegated its responsibility to the service provider. The company's board of directors has also not taken responsibility for the management of company risks.

Because there has been no exchange of information about the relevant cyber risks between Nasdaq Clearing and other parties that the company is technically connected with, the Financial Supervisory Authority assessed that Nasdaq Clearing lacked a comprehensive and comprehensive view of relevant risks. The investigation showed there was a risk management tool, however the tool to date was not used to manage cyber risks (ibid., 8).

The board of directors of Nasdaq Clearing had not defined, determined and documented the central counterparty's appropriate risk tolerance level and risk bearing capacity with regard to cyber risks. (ibid., 9).

The questionnaire showed, Nasdaq Clearing had no process, which would have made decisions about risk tolerance. Therefore, there were no clear rules how threats affect what investments to cyber security are needed. The group's risk management strategies were not anchored to the company financial plans, which means the company did not have financial contingencies for managing the risks. Finansinspektionen evaluated, that cyber risks were not covered by a risk management system as per requirement. (ibid., 10).

Finally, Nasdaq Clearing had not made any analysis of the most suitable strategy for recovery in cyber-related scenarios including IT systems being attacked or information being manipulated or corrupted. Neither were there any preparations for alternative arrangements or documentation of tested scenarios to ensure the company would be able to recover its critical functions or IT systems in a timely manner. (ibid., 10).

As a result of the deficiencies and their severity in different areas under the assessment, Nasdaq Clearing Aktiebolag was fined for SEK 25 million (ibid., 17).

7.3 Aftermath of Nasdaq Clearing case

Article 35(1)(g) of EMIR (EU Regulation No 648/2012 of the European Parliament and of the Council of 4 July 2012 on OTC derivatives, central counterparties and trade repositories) states, when outsourcing, the central counterparty shall retain the necessary expertise and resources to evaluate the quality of the services provided and to supervise the outsourced functions effectively and manage the risks associated with the outsourcing. The central counterparty shall also supervise these functions and manage these risks on an ongoing basis. (Finansinspektionen 2016b, 3).

The requirements of the article captures the essence of the issues that Nasdaq Clearing had in demonstrating with evidence that these requirements have been implemented in practice. To explain why it happened would be guess-work and the type of aftermath that does not give much justice for the case. However, to take an opposite approach and list a few things that would likely produce positive outcomes is more constructive.

By having a solid dialog with the supervising authority about the planned outsourcing arrangement and discussing the expectations and matters to consider would most likely give some pointers to requirements in EMIR and instructions. During the same dialog, the company and the supervising authority could have exchanged information on risk landscape. At that time, Finansinspektionen's risk analyses had identified cyber-attacks against financial infrastructure companies as a significant risk, in part because there was high probability, and in part because such attacks can cause extensive damage including damage to confidence in the financial markets (ibid., 4).

In addition, by taking advantage of any outsourcing guidelines and risk management frameworks or best practices would provide support on considering good principles of steering and monitoring the outsourcing arrangement.

8 EU General Data Protection Regulation and outsourcing

8.1 Scope setting

EU General Data Protection Regulation including 88 pages of articles regulating personal data protection of EU citizens presents a massive topic to cover in the first place. As this thesis is about outsourced online banking channels as a service scope, the aim of this thesis is to summarize the obligations from processor point of view in order to capture the essential topics of the interface between an outsourcing party (controller) and the vendor or supplier (processor) – mainly covered by articles 28 and from 32 to 36. This means less focus is put on describing the obligations set for the controller alone, which would be a financial institution in this case. However, some effort is given on describing privacy principles as part of compliance architecture.

Another scope limitation concerns the type of personal data in question. Online banking channels do not process any sensitive personal data such as data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, data concerning health or sex life and sexual orientation, genetic data or biometric data. There is no need under any circumstances of an online banking channel to process or persist any personal data categorized as sensitive according to EU General Data Protection Regulation.

Even though data itself is not categorized as sensitive by the regulation, the service processing context should be considered as high risk, in case the processing is about evaluation or scoring, including profiling and predicting. A concrete example of this is customer screening against a credit reference database or a company building behavioral or marketing profiles based on usage or navigation on its website (Data Protection Working Party 2017a, 8). Another example could be personal finance management service providing insight to an individuals' financials and consumer behavior. High-risk processing means a controller is subject to Data Protection Impact Assessment (DPIA) to describe and demonstrate the compliance with the regulation and address the risks (ibid., 7) assisted by relevant data processors if any.

8.2 Data protection definitions linked to thesis context

Self-service channels of outsourced online banking in Europe process personal data of data subjects, i.e. EU citizens in the role of banking customers. "Personal data" means any information relating to an identified or identifiable natural person ("data subject"); an identifiable person is one who can be directly or indirectly identified. (European Parliament and the Council of the European Union 2016, 33)

The personal data available via online banking channels is a subset of data stored in financial institutions' customer register overall. Data is processed and stored for various purposes and for example Danske Bank A/S, Finland Branch declares they process personal data for identifying and recognizing data subjects, in order to manage contact details, for risk management and securing transactions, for direct marketing, for managing e-registration, storage, reporting and replying obligations pursuant to the law and in accordance with authorities' regulations and guidelines (Danske Bank, 2018). The data is collected during the customer engagements in relationship or an application for entering into a customer relationship concerning e.g. account or credit (ibid.). Another typical scenario for a bank is to carry out payments and transfers (The processing of personal data in Mobile Bank app, 2018).

A good and concrete example of what personal data is processed by a mobile banking channel is offered by Nordea. According to their site, Nordea Mobile Bank application processes account details, payment data, name and account details of financial contacts and IP addresses in order for a customer to be able to perform banking services and for securing transactions e.g. criminal investigations (The processing of personal data in Mobile Bank app, 2018). In addition, Data Protection Working Party (2017b, 11) provides another example in the context of portability stating that a data subject's bank account can contain personal data relating to the transactions. In addition, basic contact details are typically available, such as official name, postal address, email address and telephone number.

Data Controller refers to the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of processing personal data (ibid, 33), which in this context is a financial institution offering services to customers - the data subjects. Data Processor, means a natural or

legal person, public authority, agency or other body which processes personal data on behalf of the controller (ibid, 33) and is an outsourcing partner of a financial institution providing online banking self-service channels on behalf of the financial institution. Supervisory Authority refers to an independent public authority established by a Member State pursuant to Article 51 (ibid, 35).

In addition to personal data, financial institutions and their outsourcing partners may process data known to be under banking secrecy. In Finland bank secrecy covers all non-public information that can be deemed to be of such nature that a customer or prospect customer wants to keep it confidential including the information whether a person is customer of the bank (Finanssialan Keskusliitto 2009, 1). Banking secrecy is provisioned in Finnish Credit Institutions Act. Banking secrecy predominantly addresses the security of personal data within a bank in terms of confidentiality (PricewaterhouseCoopers AG. 2017, 7). Data protection legislation goes beyond preventing the disclosure of personal data and governs the processing of personal data, provides rights to data subjects and confers duties on data controllers and processors (ibid, 7).

8.3 Outsourcing services processing personal data

EU General Data Protection Regulation imposes a number of requirements under Article 28 for controllers appointing service providers, which process personal data, including prescribing various matters which must be set out in form of a contract or other legal act. (European Parliament and the Council of the European Union 2016, 49). Processor may process the personal data only on documented instructions from the controller (ibid., 49).

A principal requirement for a controller is to use only processors providing sufficient guarantees; in particular, in terms of expert knowledge, reliability and resources to implement appropriate technical and organizational measures to comply with the regulation and to ensure the protection of the rights of the data subject (ibid., 49). To come up with such assurance, controller's due diligence should cover making of an assessment of each processor prior to entering into a processing agreement.

Sufficient guarantee could be demonstrated by a processor with help of code of conduct or certification (ibid., 56), which can be assessed by a body with appropriate level of subject-matter expertise and is accredited for that purpose by the competent supervisory authority (ibid., 58). At the time of writing of the thesis, there were neither code of conducts nor certifications available for EU GDPR. According to Pierre Chastanet (2017), Deputy Head of Unit Cybersecurity & Digital Privacy in the Directorate General for Communications Networks, Content and Technology of the European Commission, there are two codes of conduct submitted to Working Party ("WP29" – the Committee of national Data Protection Authorities) in the domain of cloud service providers and cloud infrastructure service providers; however, neither of them have been approved by Working Party ("WP29" – the Committee of national Data Protection Authorities). The progress appears slow considering that the first draft of the code of conduct on Data Protection for Cloud Service Providers was submitted in January 2015.

8.4 Subcontracting services processing personal data

The processor shall not engage another processor without prior specific or general written authorization of the controller if subcontracting also concerns processing of personal data. In the case of general written authorization, the processor shall inform the controller of any intended changes concerning the addition or replacement of other processors, thereby giving the controller the opportunity to object to such changes. (ibid.,49). EBA final draft level Guidelines on Outsourcing to Cloud is more flexible by requiring ex-ante notification to the outsourcing institution, whose consent, however, is not required (EBA 2017b, 6). Both undertaking controller and cloud service provider should have a shared understanding of which regulatory contexts are applied to which parts of outsourced services in case notification and approval processes differ depending on the service context.

8.5 Transfer of personal data to third countries outside the EU/EEA

The transfer of personal data to third countries outside the EU/EEA is a special case under EU GDPR and has a set of requirements of its own and is subject to the Commission’s adequacy decision. However, in the absence of an adequacy decision,

transfers are also allowed outside non-EU states under certain circumstances, such as by use of standard contractual clauses or binding corporate rules, where controller or processor has provided appropriate safeguards, and on the condition that enforceable data subject rights and effective legal remedies for data subjects are available (European Parliament and the Council of the European Union 2016, 62). Model contracts available at European Commission site, can be incorporated into a contract between two controllers or controller and processors assuming the main contract does not contradict with standard contractual clauses (European Council. Model Contracts for the transfer of personal data to third countries).

8.6 Scope of EU GDPR requirements from perspective of ISO 27001:2013, ISO 29100:2011 and ISO 27018:2015

8.6.1 ISO 27001:2013

EU GDPR Article 5 principle for processing personal data in a manner that appropriate security of personal data is ensured (European Parliament and the Council of the European Union 2016, 35) and Article 32 stating the controller and the processor shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate (ibid., 51) stands for all of the 114 control objectives of ISO 27001:2013 by the terms of the standard. In fact, EU GDPR text refers to certification mechanisms in general and speaks on behalf of using one by stating the Member States, the supervisory authorities, the Board, and the Commission shall encourage the establishment of data protection certification mechanisms and data protection seals and marks, for the purpose of demonstrating compliance with this Regulation (ibid., 58).

However, by applying principles of data minimization and privacy by design, and reducing the number of personal data repositories in use, financial institutions can optimize the amount of effort required to apply security controls and objectives in different solution areas. In the context of online banking channels this could primarily mean, that the channel solutions as such are stateless by design and only rely on information sources and log to a centralized security information and event management (SIEM) system.

8.6.2 ISO/IEC 27018:2014 and ISO 29100:2011

International ISO/IEC 27018:2014 standard establishes commonly accepted control objectives, controls and guidelines for implementing measures to protect Personally Identifiable Information in accordance with the privacy principles in ISO/IEC 29100 for the public cloud computing environment (ISO [ISO/IEC 27018:2014] 2014).

There is a strong correlation between EU GDPR privacy principles and those available at ISO/IEC 29100, which have been published a few years before the text of EU GDPR was agreed upon as can be seen in Table 2. However, ISO-IEC 27018:2014 as such does not cover e.g. breach notification in given 72 hour timeline or necessarily limit data transfer outside EEA although locations of processing are specified.

Table 2. Mapping of ISO 27018:2015 controls to EU GDPR privacy principles

ISO 27018:2015 controls & ISO 29100 privacy principles	EU GDPR article summary
A.1 Consent and choice	Articles 5-7, 12, 13, 14
A.2 Purpose legitimacy and specification	Purpose limitation
A.3 Collection limitation	Lawfulness, fairness and transparency
A.4 Data minimization	
A.5 Use, retention and disclosure limitation	Storage limitation Data minimization
A.6 Accuracy and quality	Accuracy
A.7 Openness, transparency and notice	
A.9 Accountability	
A.10 Information security	Accountability Integrity and confidentiality
A.10.11 Contract measures	Article 28
A.11 Privacy compliance	Article 15 Right of access by the data subject Article 16 Right to rectification Article 17 Right to erasure Article 18 Right to restriction of processing

	Article 19 Notification obligation regarding rectification or erasure of personal data or restriction of processing Article 20 Right to data portability Articles 21-22 Right to object and automated individual decision-making

9 Outsourcing to cloud and regulatory compliance

9.1 Motivation for proper supplier management

The following examples include some important lessons learned, which have drawn attention of supervisory authorities and news media; however, it is by no means a comprehensive list of public references.

Nasdaq Clearing had outsourced to the Group's parent company. However, this agreement did not contain any detailed descriptions of the relevant services or established Service Level Agreements. Furthermore, the company has not had access to information about threats, personnel situations, incident management, ongoing projects or training in cyber security. Neither has there been any information about threats related to Sweden or the Nordic region. Finansinspektionen issued a fine of 30.000.000,00 and 25.000.000,00 SEK to Nasdaq Stockholm Aktiebolag and Nasdaq Clearing Aktiebolag in 2016 due to improper outsourcing management and performance monitoring. (Finansinspektionen. 2016b, 5).

Some evidence of issues referring to interest in using standard cloud service and contracts is reported by Finansinpektionen (SWE-FSA) in its annual report from 2016; however, neither sources nor service providers are mentioned (Finansinspektionen. 2016a, 15-16). According to EBA (European Banking Authority 2017a, 15), the outsourcing institution should ensure that the contractual arrangements do not impede its competent authority to carry out its supervisory function and objectives e.g. by means of restricting access rights and right to audit the cloud service provider.

In 2015, Swedish Transport Agency outsourced their IT-services to IBM Sweden. The contract process was speeded up bypassing some laws and internal procedures

resulting in having people abroad without proper security clearance, handling servers with sensitive materials (Reuters 2017). According to Stefan Lofven, Swedish Prime Minister, his country and its citizens were exposed to risks by potential leaks of sensitive material. Maria Agren, a former director-general of the transport agency, was fired in January for undisclosed reasons and was fined for 70,000 SEK for being careless with secret information (Financial Times 2017).

9.2 Overview of outsourcing guidelines

There are three key guidelines published by European Banking Authority (EBA) from the outsourcing, outsourcing to cloud and ICT outsourcing risk management perspective.

EBA SREP guideline is intended to promote common procedures and methodologies for the assessment of the Information and Communication Technology (ICT) risk under the Supervisory Review and Evaluation Process (European Banking Authority 2017b, 3). The guideline is meant for the guidance of competent authorities but can be used in reverse, e.g. to internally validate if there is proper governance framework in place to *among other things* implement ICT strategy, and management body is capable of addressing the risk associated with the ICT (see ibid., 15). SREP guideline provides also an annex (see ibid., 32-37) of risk categories, risks and examples, which can be considered as financial institution's own risk assessment.

The Committee of European Banking Supervisors' Outsourcing guideline (2006) describes general provisions for outsourcing covering due diligence, contract, SLA, contingency and exit planning, and according to CEBS, e.g. in order to promote greater consistency of approach in EU where possible
within the national legal frameworks (Committee of European Banking Supervisors 2006, 1). The guideline has been totally transposed by 54% and 38% partially within EU member states (EBA 2017a, 21).

Finally, the main objective of the guideline Recommendations on Outsourcing to Cloud Service Providers under Article 16 of Regulation (EU) No 1093/2010 (European Banking Authority 2017a, 22) is to:

Specify a set of principle-based rules that complement and update the CEBS guidelines for competent authorities to apply in their regulatory and supervisory framework for the cloud outsourcing process and the associated risks

The recommendations for outsourcing in cloud highlights that many of the provisions set in CEBS are still effective also in cloud, but makes a few revisions excluding requirement of prior consent in case changes to subcontracting and by enabling pooled audits (European Banking Authority 2017a, 24).

It is good to remember, that these guidelines directly refer to other regulatory contexts as well, such as data protection. Table 3 illustrates the key outsourcing guidelines, their primary target audience and application date.

Table 3. List of compliance guidelines and effective dates

Author and guideline	Primary target audience	Secondary or indirect audience	Effective date
EBA - Guidelines on ICT Risk Assessment under the Supervisory Review and Evaluation process (SREP)	competent authorities, auditors	financial institutions	1.1.2018
EBA - Guidelines on outsourcing to cloud	competent authorities , financial institutions, auditors	cloud service providers	June-2018
EBA - CEBS outsourcing guidelines	competent authorities , financial institutions, auditors	outsourcing service providers	2006
Finanssivalvonta - Ulkoistaminen rahoitussektoriin kuuluvissa valvottavissa	financial institutions, auditors	outsourcing service providers	2012
Finansinspektionen's Regulations and General Guidelines regarding information security, IT operations and deposit systems	financial institutions, auditors	outsourcing service providers	2014

It is expected that Finansinspektionen will publish more instructions soon. SWE-FSA has announced “EBA will shortly publish EU common cloud services guidelines. FI has participated in that work and plans to return further guidance with reference to these guidelines.” (Finansinspektionen, 2017b).

9.3 Short history of outsourcing regulations

The current guideline on outsourcing for banks and investment institutions is from the Committee of European Banking Supervisors (CEBS) predecessor, European Banking Authority and dates back to 2006, the same year when Amazon launched its Elastic Compute cloud (EC2), which allowed companies and individuals to rent scalable computing capacity. According to Baker McKenzie (2017, 2006 CEBS Guidelines), the volume of financial information, data and demand for outsourcing to cloud service providers has increased substantially since then.

Keeping in mind the evolution of cloud computing during the past decade and the fact that EBA has not made any distinction between outsourcing and outsourcing to cloud, it comes as a no surprise there is a high level of uncertainty regarding the regulatory provisions, forming an obstacle in the adoption of cloud services (European Banking Authority 2017a, 5). The major benefits from establishing a common European framework for outsourcing are reduction in operational risk, level playing field across competing institutions in regards to regulative burden and supervisory convergence (ibid., 24).

The final report on recommendations on cloud outsourcing has some eight pages of recommendations excluding from the count any background information, executive summary, rationale and accompanying documents, which means the paper’s core content is relative short and easy to read through, although there are plenty of references to CEBS guideline, which should be considered as a supplementary document for outsourcing in general. More effort is required to internalize the obligations and cost elements in it in depth and the relationship to information security overall – what is in the focus area and what is not directly touched upon. The outline of the content of the paper is illustrated in Figure 4.

Figure 4. Outline of the draft recommendation on outsourcing to cloud (taken from presentation of European Banking Authority at public hearing 20.06.2017)

9.4 ICT outsourcing risks and risk profile factors

To understand in-depth the compliance requirements set by European Banking Authority, one approach is to understand the risk profiles, risk categories and threat landscape having a prudential impact. By average, some 20 online banking incidents occurred in Finland, which were reported during years 2013 and 2014 (YLE 2015). The overall number of disturbances reported to Finanssivalvonta (FIN-FSA) is much higher and was on the level of 122-155 on a yearly basis between 2013 and 2015 (YLE 2016). Markku Koponen from Finanssivalvonta states in the same article that Finnish bank's online channels are reliable. It is typical, that any disturbances noticeable to end customers concerning online banking channels are newsworthy, which increases the criticality of the channel services.

European Banking Authority Guidelines on ICT Risk Assessment under the Supervisory Review and Evaluation process (SREP) set out the requirements, that the competent authorities should apply in their assessment of ICT focusing on the general provisions and application of scoring as part of the SREP assessment of risks to capital, assessment of institutions' governance and strategy on ICT and assessment of institutions' ICT risk exposures and controls. (EBA 2017b, 3). These

guidelines include also assessing the risks related to ICT outsourcing. The material related to ICT outsourcing can be found helpful to validate if certain risk scenarios have been thought of and their criticality level of ICT systems and services classified.

SREP introduces its own risk taxonomy for authorities as a step forward in establishing a link between the concepts and concerns of complex, detailed and highly technical IT audit frameworks, e.g. Cobit, CMMI and ISO, and the guidelines EBA offers (EBA 2017b, 46). EBA justifies its approach that the standards are little known and understood by non-IT experts and there is demand for more practical and intuitive language and thinking frameworks by supervisors. Financial institutions have the freedom to maintain their own risk taxonomies (ibid., 76).

9.5 Definition of critical ICT system or service

SREP has a definition for a critical ICT systems and services also referring to the context of this thesis. According to the guideline (EBA 2017b, 20), ICT system or service is critical if they support:

> *core business operations and distribution channels (e.g. ATMs, internet and mobile banking), essential governance processes and corporate functions (e.g. risk management and treasury), they fall under special legal or regulatory requirements, they process or store confidential or sensitive data to which unauthorized access could significantly impact (e.g. databases), they provide vital base line functionalities (e.g. telecom, connectivity, ICT and cyber security services).*

In light of this definition, a single online banking channel in a multi-channel environment would not be considered critical because of having the role of complementing service channel. A single channel has neither significance from shared core or baseline functionality point of view assuming there are no cross-dependencies between the online channels. However, an online banking channel for authenticated customers typically does process confidential or sensitive data. Unauthorized access could have significant reputational and regulatory impact. Execution of fraudulent payment transactions by hackers through the breaking or circumvention of the security of e-banking and payment services and/or by attacking

and exploiting security vulnerabilities in the internal payment systems of the institution was given as a related ICT security risk in ICT Risk Taxonomy Annex (EBA 2017b, 33). Due to reputational impacts and the risk profile, internet and mobile banking channels should be considered material and critical ICT systems by definition.

Assuming the channels were operated from a single operative environment, the online banking channel could have common dependencies between all the customer-facing channels, which would also be interpreted as critical due to serving core business operations and distribution channels. An example implementation of this type of component could be an enterprise service bus providing e.g. message transformation services and service APIs for surrounding system landscape.

9.6 ICT outsourcing risks

The introduction of a white paper by Haller and Wallen (2016, 1) describes that outsourcing to third parties and the resulting dependency risks have become a leading consideration for financial services firms, drawing extensive management attention and regulatory scrutiny. Attackers know that third party suppliers can be a weak link and target them to gain foothold on infrastructure of a financial institution (ibid., 1).

SREP guidelines acknowledge this type of scenario within ICT outsourcing risk category illustrated in Figure 5. The list is stated not to be exhaustive, but aims to bring about a uniform understanding of risk categories and facilitate a common language (EBA 2017b, 76). Some level of emphasis should be given to the examples that ended up in the annex, regardless of the fact that these guideline documents are not necessarily meant to be correlated against each other. It should be fair to say, that for the sake of consistency and focusing resources effectively, the risk categories, risk descriptions and examples should be the primary concerns of both authorities and financial institutions.

ICT risk categories	ICT risks (non exhaustive[13])	Risk description	Examples
	models or data dictionaries	models or data definitions, and/or differences in the underlying data generation and change process.	the level of the whole financial institution or group.
ICT outsourcing risks	Inadequate resilience of third party or another Group entity services	The non-availability of critical outsourced ICT services, telecommunication services and utilities. Loss or corruption of critical/sensitive data entrusted to the service provider	• Unavailability of core services as a result of failures in suppliers (outsourced) ICT systems or applications. • Disruption of telecommunication links. • Power supply shortage.
	Inadequate outsourcing governance	Major service degradation or failures due to inefficient preparedness or control processes of the outsourced service provider. Ineffective outsourcing governance may result in a lack of appropriate skills and capabilities to fully identify, assess, mitigate and monitor the ICT risks and can limit institutions' operational capabilities.	• Poor incident handling procedures, contractual control mechanisms and guarantees built into the service provider agreement that increase key man dependency on third parties and vendors. • Inappropriate change management controls concerning the service provider ICT environment can cause major service degradation or failure.
	Inadequate security of third party or another Group entity	Hacking of the third party service providers' ICT systems, with a direct impact on the outsourced services or critical/confidential data stored at the service provider. Service provider staff gaining unauthorised access to critical/sensitive data stored at the service provider	• Hacking of service providers by criminals or terrorists, as an entry point into the institutions' ICT systems or to access /destroy critical or sensitive data stored at the service provider. • Malicious insiders at the side of the service provider try to steal and sell sensitive data.

Figure 5. ICT outsourcing risk taxonomy of SREP (European Banking Authority 2017b, 37)

The risks named in the Annex of the guidelines (ibid., 37) cover service resiliency, outsourcing governance and information security. The outsourcing to cloud (European Banking Authority 2017a, 16) in Chapter 4.5 and CEBS guidelines (Committee of European Banking Supervisors 2006, 6) address resiliency only by stating that institutions should implement arrangements to ensure the continuity of the services provided by the outsourcing service provider. The accuracy and concreteness level of audit guideline is more fine-grained than the actual set requirements. The same issue continues with change management and malicious insiders, which are identified as example risks but are not referred directly at all in the outsourcing guideline.

In addition to outsourcing risks, there are risk categories, which are relevant from the online banking context point of view, and which directly refer to e-banking, such as: ICT availability and continuity risks including distributed denial of service against e-banking services; ICT security risks, and e.g. circumvention of security of e-banking and payment services for execution of fraudulent payment or securities transactions (European Banking Authority 2017b, 32-33).

9.7 Outsourcing and cloud delivery models

In the draft version of the EBA recommendation, definitions were given to cloud services, public, community, hybrid, private cloud and IaaS, PaaS and SaaS delivery models (see European Banking Authority 2017a, 10-11), which are introduced in the

context of requirement of having a registry including the information of the type of cloud and its delivery model (ibid., 13). The fact that there was no reference to commonly used definitions such as NIST or a distinction between cloud service provider and resource operator was criticized by Temenos, a financial service company based in Switzerland, in its reply to the consultation paper (Temenos 2017, 1-2). The lack of further reference to types of cloud or cloud delivery models suggest the types and models are treated as equal as long as all requirements are met including the ones touching upon chain outsourcing and subcontracting.

Finansinpektionen has stated in its yearly report from 2016 (Finansinspektionen 2016a, 15) that it does not make a distinction between outsourcing to cloud and traditional forms of outsourcing to an IT supplier. It is up to the company risk management to evaluate and make sure the information security risks are under control (ibid, 15). In comparison of Finansinspektionen's statement from 2016 with EBA's new recommendation on outsourcing to cloud, the latter will provide more practical and hands-on approach to outsource contracting on cloud trying to ensure that financial institutions consider the most common pitfalls from risk management point of view.

9.8 Content analysis of recommendation on outsourcing to cloud service providers

The following chapter describes the approach taken to understand the requirements outlined in the recommendation in depth. A process description was done from both financial institution and supplier perspectives based on the information given in the outsourcing guideline to illustrate the effort and regular activities required in the compliance process.

To summarize the recommendations, ISO-IEC 27001 reference control objectives and controls list was used to gain understanding to which categories the requirements of the recommendation fall into in an information security system. In practice all of the requirements could be primarily classified under Compliance (A.18) control due to originating from an authority. However, the latter approach, where all the

requirements are classified under compliance, would not bring any further insight in which security domains and control objectives should be considered.

The auditing guidelines of SREP for competent authorities were compared against the requirements for outsourcing institutions. Even though the publisher is the same entity (European Banking Authority), inconsistencies between expectations were identified.

9.8.1 Summarization and classification of outsourcing requirements

The summarization in Appendix 1 is done from the perspective of a financial institution, therefore requirements from 10 to 13 were opted out. In total, there were 23 unique requirements for financial institutions, four (4) for cloud service providers and four (4) as well for competent authorities. Requirement number 15 counted as two separate requirements, which are directly overlapping with provisions already set in CEBS Guideline. Requirement number 4 and 5 were joined due to number five (5) only providing clarifications to the previous one. The consistency of numbering of the requirements in the draft version of the recommendations still seems to be under work. Figure 6 illustrates the number of requirements in each category of ISO-IEC 27001 reference control objectives and controls; most of the requirements fall under supplier relationships category.

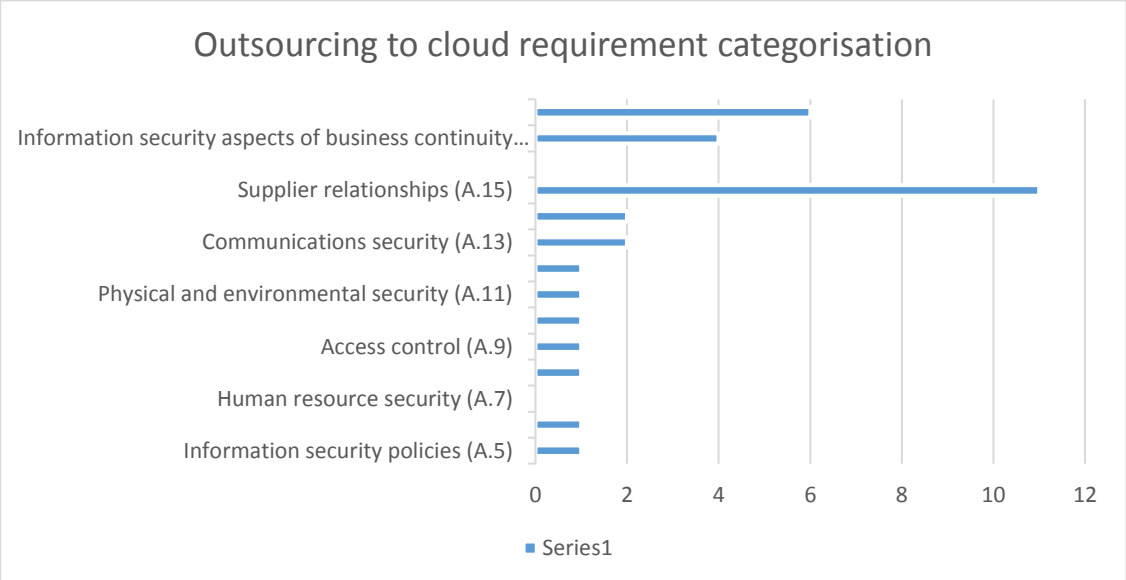

Figure 6. Outsourcing to cloud requirement categorization

Table 4 below illustrates the forms, in which the outputs or evidence of the activities required from a financial institution by European Banking Authority could be described based on cites from EBA recommendations.

Table 4. Outputs and evidence of compliance required by EBA recommendation on outsourcing to cloud service providers based on interpretation

Document	**Requirement**	**Definition**	**Evidence or success criteria**
Materiality assessment	Requirement 1, Chapter 4.2	To demonstrate financial institution has understood the risk impacts from business perspectives and considered	Analysis of items from 1A to 1D of the guideline covered in the documentation
Outsourcing register	Requirement 4, Chapter 4.2	Register with information related to all its material and non-material outsourced activities at institution and group level	Information requested in requirement 3 and 4 available and documented per request by NFSA
Contingency and exit plan	Requirement 26, Chapter 4.8	Contingency planning and clearly defined exit plan	Documented, sufficiently tested
Transition plan	Requirement 27 b, Chapter 4.8	Identify alternative solutions and develop transition plans to be able to remove and transfer existing activities and data from the CSP to these solutions	Documented, sufficiently tested in a controlled way taking into account data location issues and maintain business continuity during the transition phase
Outsourcing contract	Requirement 15, Chapter 4.5		
Service Level Agreement	Requirement 15, Chapter 4.5		
Internal or 3rd party audit report	Requirement 8, Chapter 4.3		Audit report
Certification by 3rd party	Requirement 8, Chapter 4.3		Audit report

9.8.2 Changes to outsourcing requirements introduced by cloud recommendations

In comparison to the previous outsourcing guideline by CEBS, the new version by European Banking Authority, there are a few new requirements extending the basic scope of more traditional outsourcing context.

One of these is the requirement for the outsourcing institution to maintain an updated register of information on all its material and non-material activities that are outsourced to cloud service providers at institutional and group level, including information of description of the activities and data to be outsourced, applicable law governing the contract and the country or countries where the service is to be performed (European Banking Authority 2017a, 12).

By definition in CEBS (CEBS 2006, 2-3) guideline, material activities have such an importance that:

- any weakness or failure in the provision of these activities could have a significant effect on the financial institution's ability to meet its regulatory responsibilities and/or to continue in business,
- any other activities requiring a license from the supervisory authority,
- any activities having a significant impact on its risk management,
- and the management of risks related to these activities.

Where an outsourcing institution does not employ its own audit resources, it can consider using new tools such as pooled audits or third-party certifications, third party or internal audit reports made available by the cloud service provider (European Banking Authority 2017a, 14). This can help financial organizations to get synergies from previous auditing efforts and burden the cloud service providers less.

Prior consent is no longer required for changes in subcontracting, though the outsourcing institution and the cloud service provider should specify any types of activities excluded from potential subcontracting and indicate that the cloud service provider retains full responsibility for and oversight of those services that it has subcontracted (European Banking Authority 2017a, 17). There are also more details on requirements to make a risk assessment in case of changes to subcontracting based on information received from a CSP and requirement to monitor outsourcing

performance regardless of whether the service or parts of it are provided by the cloud service provider or its subcontractors (ibid., 18).

In addition, the recommendations include guidance implementing adequate controls and measures on the data security in risk based manner, such as the use of encryption technologies for data in transit, data in memory and data at rest (ibid., 3). However, considering that similar expectations are already set by European Data Protection Regulation, this should not introduce an additional cost element for the financial institutions.

9.8.3 Costs incurring from outsourcing to cloud recommendations

This chapter describes the direct cost elements of post-contractual phases of outsourcing recommendations. There are also indirect costs from decision making, due diligence checks on cloud service provider, requirement setting and contract negotiations, which are considered to belong to pre-contractual or contractual phases.

There are two types of competence related cost elements present in the guidelines, in addition to understanding of outsourcing and compliance issues in the type of arrangements in general, assessing risks and maintaining the skills and resources necessary to adequately monitor the outsourced activities.

CEBS guideline, which should be read in conjunction with outsourcing to cloud recommendations, state that outsourcing institutions should retain adequate core competence in-house at a senior operational level to enable them to have the capability to resume direct control over an outsourced activity in an extreme situation (CEBS 2006, 3).

Considering the high level of technical complexity of cloud solutions, the outsourcing institution should verify that the staff performing the audit, or the staff reviewing the third-party certification or service provider’s audit reports, have acquired the right skills and knowledge to perform effective and relevant audits and/or assessments of cloud solutions (European Banking Authority 2017a, 14-15).

Testing of exit strategy is required by European Banking Authority, where appropriate, whether it is in the form desktop exercise, live testing or some other

form, can have a cost impact especially if any third parties are involved in testing (European Banking Authority 2017a, 68).

In addition to competences, there are process level cost elements related to risk management, keeping and maintaining cloud outsourcing registry, auditing or assessing available audit reports by CSP, monitoring of SLA and key performance indicators as well as management of an outsourcing arrangement including following up the changes affecting the outsourcing service provider, e.g. major change in ownership, strategies, profitability of operations.

Finally, the outsourcing contract itself might introduce some additional fees which are not part of standard service but are required to have privileged audit and access rights for contractual compliance.

9.9 Outsourcing to cloud and supplier management processes

The process description of risk management prior to outsourcing agreement of a financial institution could be illustrated as Figure 7 based on SREP Controls for managing material ICT outsourcing risks (European Banking Authority 2017b, 29) and chapter 4.1 of Recommendations on outsourcing to cloud service providers (European Banking Authority 2017a, 12).

It could be claimed that the critical success path is to ensure a level of information security and outsourcing knowledge, produce the information or evidence in form of documents required by relevant outsourcing recommendation, engage supervisory authority from the start to validate the plans and documents, draft and sign a contract considering compliance obligations and follow-up the delivery of service by means of performance and risk monitoring.

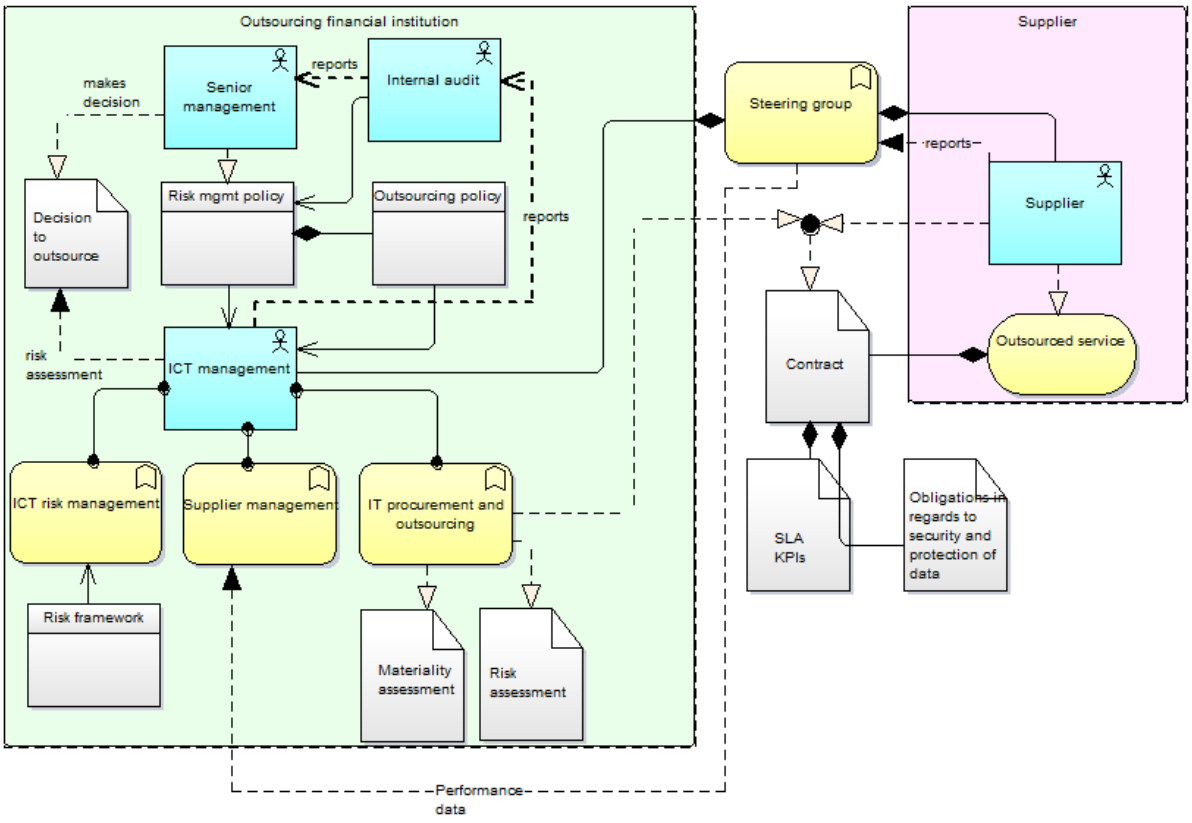

Figure 7. Outsourcing to cloud and supplier management processes

The recommendations or requirements can yet be categorized to three stages: 1. steps to carry out prior outsourcing standing for material assessment and ex-ante notification; 2. commercial negotiations to ensure contractual obligations; 3. performance and risk monitoring and continuous improvement during continuous service phase. The three-staged process illustrated by EBA can be seen in Figure 8.

This illustration does not dive into implementing the actual service setup by cloud service provider based on security and data protection obligations.

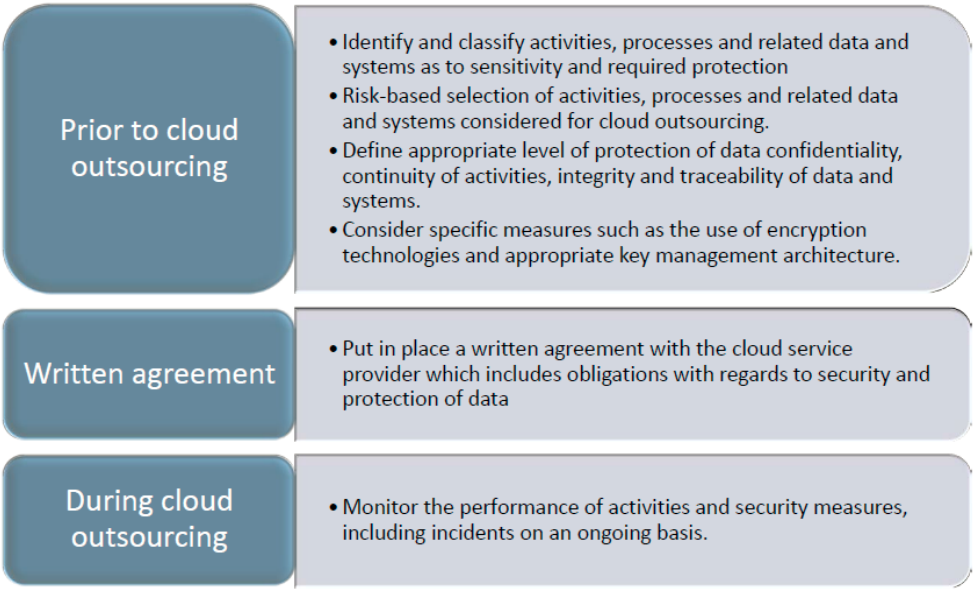

Figure 8. Three phases of outsourcing (taken from presentation of European Banking Authority at public hearing 20.06.2017)

10 Compliance solution architecture

10.1 Overview

The compliance solution architecture proposed by this thesis consists of collections of controls and principles from different concreteness level of regulations, provisions, guidelines, recommendations, although those documents are typically principle-based rather than contain detailed requirements in order to avoid the need for constant updating.

It is, however, noteworthy that there can be gaps in the type and depth of controls, which are identified by outsourcing or data protection related documents from European Council and European Banking Authority, in comparison to industry best

practices. For example, the depth of controls hardly ever reaches the level of application software like OWASP Application Security Verification Standard (ASVS).

In overall, as suggested also in the introduction chapter, the compliance architecture of online banking self-service channels could consist of capabilities and artifacts such as:

- contracts,
- information security and outsourcing or service management processes,
- technical architecture and capabilities,
- and skills and knowledge for operating the service context.

The sub-chapters cover more of the

- principles having impact on type of security controls required,
- non-functional requirements for the architecture,
- functional requirements for online bankin channels,
- and contractual requirements supported by automated capabilities to produce SLA reporting.

The process level requirements are covered in Chapter 10 where risk management is one of the focus areas. Knowledge and skill related requirements have not been specified in the thesis.

10.2 Security principles

10.2.1 Data privacy by design and by default

Both European Parliament and the Council of the European Union (2016, 6) and ISO/IEC29100 (2011, 9) embrace the concept of Privacy by Design meaning reducing the risk of collecting unsolicited PII by considering privacy safeguarding measures starting at the time of the design of the system throughout the entire information life cycle end-to-end.

> Such measures could consist, among other things, of minimizing the processing of personal data, pseudonymising personal data as soon as possible, transparency of the functions and processing of personal data, enabling the data subject to monitor the data processing, enabling the controller to create

and improve security features. (European Parliament and the Council of the European Union 2016, 15).

The definition of Privacy by Design is not just about adoption and integration of privacy-enhancing technologies (PETs) type of elements but spans to a variety of settings of application covering from information technology to business practices, physical design and infrastructures (European Commission, 2018).

To be able to demonstrate, that data privacy by design and by default is embedded in line with the principle of accountability in Article 5 (European Parliament and the Council of the European Union 2016, 36) into the design, operation and management of a given system landscape forming a set of business processes, certification can be seen as effective and practical approach unless considered as a founding requirement.

10.2.2 Lawfulness, fairness, transparency and purpose limitation of personal data

EU GDPR requires, that personal data of a data subject shall be processed lawfully, fairly and in a transparent manner, collected for specified, explicit and legitimate purposes and not further processed in a manner incompatible with those purposes (European Parliament and the Council of the European Union 2016, 35).

10.2.3 Accuracy of personal data

EU GDPR requires, that personal data of a data subject shall be accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, regard to the purposes for which they are processed, are erased or rectified without delay (European Parliament and the Council of the European Union 2016, 35).

10.2.4 Data minimization

Personal data must be collected for specified, explicit and legitimate purposes and must be adequate, relevant and not excessive in relation to the purposes for which it is collected and/or further processed (European Parliament and the Council of the

European Union 2016, 35). Even though many of the interactions between online banking channels and dependency systems typically lead to exchange of more data than is required by the end user process, not all the data is relevant to be stored by the online banking channel. In fact, the context should be understood only as a gateway for processing the data, not as a master in terms of data persistence, which means there is an emphasis on securing the data exchange between the channel and dependency systems such as identity and access management system, customer relationship management (CRM), core banking (accounts, loans), security information and event management (SIEM), web analytics, customer messaging and so forth.

10.2.5 Principle of least privilege and security in depth

According to EBA Guidelines on ICT risk under the Supervisory Review and Evaluation process under the controls for managing material ICT security risk, the assessment of competent authorities should validate if a financial institution's ICT security policy takes into account the principle of least privilege (i.e. limiting access to the minimal level that will allow normal functioning for access right management) and principle of defense in depth, which stands for layered security mechanisms increasing security of the system as a whole for designing a security architecture. (European Banking Authority 2017b, 27).

10.2.6 Segregation of duties

Financial institution's risk control framework should consider specifications regarding the required segregation of duties during the different phases of the implemented ICT change processes with a focus on the implemented solutions and segregation of duties to manage and control changes to the production ICT systems and data by ICT staff or any other party (European Banking Authority 2017b, 28).

10.2.7 Right to audit

The right to audit is a key right laid down in the principles of the CEBS guidelines (European Banking Authority 2017a, 6). To reduce the manual effort, involvement and need for a physical access during audit, the system should support logical access

and virtual audit of the data for the financial institution and supervising authority. Because of the fact that outsourcing institutions have the flexibility to exercise these rights in a risk-based manner by e.g. relying on third-party audit reports or certifications according to EBA (European Banking Authority 2017a, 47), certification against a well-known standard can be seen as a method to streamline and reduce costs of auditing.

10.3 Data anonymisation, pseudonymisation and tokenization techniques

The following techniques are recognized by Data Protection Working Party (2014, 21) in terms of security measures enhancing data privacy illustrated in Figure 9 describing whether 1) identification of an individual in the dataset 2) linking two records assigned to a same group of individuals but without capability to single out individuals 3) or the possibility to deduce a value of an attribute from the values of a set of other attributes in dataset, is still possible after use of corresponding technique. It is worth mentioning that each of these techniques fail to meet with certainty the criteria of effective anonymization, i.e. processing of personal data in order to irreversibly prevent identification.

	Is Singling out still a risk?	**Is Linkability still a risk?**	**Is Inference still a risk?**
Pseudonymisation	Yes	Yes	Yes
Noise addition	Yes	May not	May not
Substitution	Yes	Yes	May not
Aggregation or K-anonymity	No	Yes	Yes
L-diversity	No	Yes	May not
Differential privacy	May not	May not	May not
Hashing/Tokenization	Yes	Yes	May not

Figure 9: Strengths and Weaknesses of the Techniques Considered (Data Protection Working Party 2014, 24).

Tokenization technique is typically applied but not limited to in the financial sector to replace card ID numbers by values with reduced usefulness for an attacker. The

values are typically derived by the use of one-way encryption mechanisms or the assignment, through an index function, of a sequence number or a randomly generated number that is not mathematically derived from the original data. (ibid, 21). Another use case is to exchange user authentication or identification information during the login process to a technical customer-id, which is used to link customer data to the data subject, however, it is only known by the processing system and not shared with the data subject. This type of system design assumes customer-id is shared by all dependency systems, or those at least have the capability to make a subsequent call to exchange a tokenized id to an id recognized by the system. Additional calls have a performance impact on overall system design.

10.4 Portability in cloud outsourcing strategy

As Dutch Banking Association (Nederlandse Vereniging van Banken) suggests in its response to EBA consultation paper of draft recommendations on outsourcing to cloud service providers, it is important that financial institutions take responsibility and plan how they distribute their business critical systems. Having more than one cloud service provider and having bank critical applications able to run on multiple clouds at the same time may prove to be critical for their survival. (Dutch Banking Association, 2017). Looking at this from a different angle means a supplier or a cloud service provider of a financial institution should avoid use of solution components, which rely on technology introducing vendor-lock-in level dependencies. Portability can be seen as a good architectural design principle contributing to contingency planning and exit strategy.

10.5 Resiliency in cloud

Cloud Security Alliance (CSA response to European Banking Agency consultation paper on outsourcing to cloud service providers, 2017) states that resilience can be achieved in many different ways e.g. by use of availability zones and the like in a single cloud provider context as well as architectures designed to be fault tolerant by consuming multiple CSP offerings across cloud providers beyond one SLA delivery promise. Cloud Security Alliance believes multi-sourcing of CSPs in combination with resilient architectures is the deployment model for systemically important services,

reducing concentration risk and making exiting a provider less disruptive due portability. Neither the outsourcing guidelines nor data protection regulation have any references to system resiliency from requirement setting point of view, instead outsourcing guideline embraces the topic on higher level by referring to business continuity overall.

10.6 Security controls

10.6.1 Intrusion detection, prevention and vulnerability management

EBA Guidelines on ICT risk under the Supervisory Review and Evaluation process (European Banking Authority 2017b, 27) instruct competent authorities to assess the protection of critical ICT systems and services by seeking evidence of adoption of for example a vulnerability assessment process, software patch management, end point protection (e.g. malware virus), intrusion detection and prevention tools. In general, processes and solutions to secure websites and applications include a combination of recognized secure development practices, ICT system hardening and vulnerability scanning practices, implementation of additional security solutions such as application firewalls, intrusion detection (IDS) and/or intrusion prevention (IPS) systems (ibid., 28).

10.6.2 Logging and reporting

Financial institutions are expected to have controls for user and administrative activity logging part of managing material ICT security risks (European Banking Authority 2017b, 25). User and administrative activity logging serve the purpose of enabling effective monitoring and the timely detection and response to unauthorized activity, e.g. to assist in or to conduct forensic investigations of security incidents (European Banking Authority 2017a, 26).

Neither outsourcing guidelines nor data protection regulation further elaborates the architecture for logging or how to protect audit logs from modification and to maintain integrity of the logs. However European Payments Council (2010), an international not-for-profit association and not a part of the European Union institutional framework, has published a comprehensive document of principles and

best practices for banks under title ‘The use of audit trails in security systems: guidelines for European banks’ in 2010.

As this document is beyond the scope of this thesis, complete information about the 50 principles introduced by the guideline are not addressed here, however, there are two principles worth mentioning here. According to EPC Principles 7 and 9, organizations should consider the use of a Security Event Management or SIEM system due to the large volume of security events (European Payments Council 2010, 11). A system of this scale should be considered to be by nature a generic and shared component of enterprise’s architecture rather than limited to the architecture of online banking channels. Another important principle is to protect of the integrity of audit logs from any modification by e.g. signing the logs with digital signatures or by sending logs to write-once type of media (ibid., 14).

10.6.3 Key management and data encryption

There are only few architectural or technical requirements for financial institutions in the outsourcing guidelines, however, the one seen worth mentioning in the final draft version of outsourcing guideline to cloud is, that specific measures should be considered where necessary, such as the usage of encryption technologies in combination with appropriate key management architecture for data in transit, data in memory, and data at rest (European Banking Authority 2017a, 16).

EBA has not refined the requirements any further but to protect against both an external breach of the service provider as well an attack originating from a privileged user or employee of the provider. For example Cloud Security Alliance (2012, 10) promotes the principle of segregation of duties and separating key management from the cloud provider hosting the data. In addition IBM’s (2017) reply to the consultation paper recommends, that whilst encryption remains an outsourcing institutions choice, the client should maintain independent control of the encryption keys.

From online banking architecture’s point of view, the end user traffic must be secured over TLS connection even if outsourcing guidelines or EU GDPR use terms such as ‘where necessary’, ‘may’, ‘such as’ and ‘as appropriate’ indicating

encryption a security control, which is strongly advised but not enforced. OWASP (2017) strongly advices, that if the web application handling sensitive data may be the target of determined attackers, to use TLS services everywhere, whether the implementation is based on software library or a hardware device, provided by FIPS 140-2 validated crypto modules adding a layer of physical security requirements over FIPS 140-1.

Data protection in rest and in memory are more closely connected to capabilities and technologies being involved and offer less surface on discussing the topic from a broader perspective. It can be said that there are more COTS products for data at rest encryption, which can be implemented on e.g. a file system or natively on database engine level compared to available solutions for data in memory encryption.

Data in memory encryption is by nature more tightly coupled with processor architecture. For example, AMD technology integrates the main memory encryption capabilities with virtualization architecture and can be used in both cloud and Docker type models. Solutions at this level are transparent to software. (Kaplan & Powell & Woller 2016, 2)

10.6.4 Denial of service protection

EBA Guidelines on ICT risk under the Supervisory Review and Evaluation process expects evidence of solutions to protect critical internet activities or services (e.g. e-banking services) where necessary and appropriate, against denial of service attacks from the Internet, aimed at denying or disturbing access to these activities and services. (European Banking Authority 2017b, 26).

10.7 Operationalizing of data subject rights

10.7.1 Terms and conditions and consent management

An online banking channel should have settings for data subject's acceptance of the proposed processing of his or her personal data. Silence, pre-ticked boxes or inactivity does not constitute a consent according to EU GDPR (European Parliament and the Council of the European Union 2016, 6). The consent should be formulated

by the controller in an intelligible and easily accessible form using clear and plain language, and it should not contain unfair terms (ibid., 8). The data subjects should be made aware of risks, rules, safeguards and rights in relation to the processing of personal data and how to exercise their rights in relation to such processing (ibid., 7), which simply put means the data controllers must inform the data subjects about their different rights under the regulation.

10.7.2 Settings for processing personal data for marketing

In EU GDPR Article 21, data subject shall have the right to object at any time to processing of personal data for such marketing that includes profiling related to direct marketing. If objected, the personal data of the individual shall no longer be processed for such purposes. (European Parliament and the Council of the European Union 2016, 45).

10.7.3 Restriction of processing

EU Data Protection Regulation Article 21 states the data subject has the right to obtain restriction of processing from the controller when specific conditions are met such as the controller no longer needs the personal data for the purposes of the processing. However, they are required by the data subject for the establishment, exercise or defense of legal claims, or in case the accuracy of the personal data is contested by the data subject (European Parliament and the Council of the European Union. 2016, 45).

This data subject right can be interpreted as if the Front Office channels, supporting the customer facing online banking channels, should have the option to flag an end customer with status of restriction of processing as well as restricting further processing of personal data until the restriction is lifted.

10.7.4 Right to be forgotten and data portability

With the assumption that the online banking channels are implemented stateless, there should be no need to have a far-fetched process for deleting customer data. However, in case there is some personal data stored, by minimum there should be an API that could interact with master exit process of customer of a financial institution.

The same applies to data portability except that online banking channels can be considered as the most convenient media for requesting and delivery of portable personal data in electronic format, e.g. account statements.

10.8 Outsourcing contract and EU GDPR compliance

As a due diligence requirement, EU Data Protection Regulation requires, the controller should use only processors providing sufficient guarantees, in particular in terms of expert knowledge, reliability and resources, to implement technical and organizational measures for the security of processing (European Parliament and the Council of the European Union. 2016, 49).

A written contract or other legal act stipulates that the processor processes the personal data only on documented instructions from the controller that applies as well to transfers of personal data to a third country or an international organization (ibid., 49).

10.9 Service level reporting

Outsourced service architecture must technically implement the quality and performance criteria metrics measured on agreed intervals and with history of review period correlating with what was written onto outsourcing contracts and about agreed service levels. Service level agreement (SLA) describes the minimum expected level of service and set of key performance indicators to be followed during the outsourcing contract implementation. Quality and performance criteria should also cover security for a financial institution to be able to monitor and manage the risks associated with its outsourcing arrangements on on-going basis. (European Banking Authority 2017a, 16).

Typical key performance indicators (KPI) for an online service is service availability and response time per agreed time unit, which have direct impact on end-user experience. The PKIs should be aligned with the strategic objectives of the company. Table 5 outlines examples of PKIs for banks to be considered as part of an SLA by Federal Deposit Insurance Corporation (2014) that published a document intended

to serve as a resource for banks in addressing specific challenges relating to technology outsourcing.

Table 5: Examples of SLA objectives, requirements and measurements (Federal Deposit Insurance Corporation 2014, 6).

TABLE 1 – EXAMPLES OF OBJECTIVES, REQUIREMENTS, AND MEASUREMENTS

Strategic Objective	Performance Requirement	Measurement
Sensitive system and bank/customer data must be protected with strong security.	Regular checks for intrusions or other security breaches.	Copies of intrusion scan reports to be sent at pre-determined frequency.
	Periodic security assessments, tests, or reviews.	Copies of independent security assessment reports to be provided at pre-determined frequency.
	Timely reporting of incidents and follow up to bank management.	Regular incident reports (frequency will depend upon system criticality).
Mission critical systems must be reliable and accessible.	System downtime must be minimal.	Specified requirement for system uptime (e.g., 99.9%).
	The system must be able to support certain volumes of activity at a given time.	Specified requirement or parameters for capacity (e.g., 1,000 transactions processed per minute).

11 Compliance risks and business blockers of cloud adoption and for cloud architecture

11.1 Insufficient knowledge of outsourcing to cloud and auditing

Outsourcing a material service to a third party is a risk from multiple perspectives in case the outsourcing party does not have sufficient competence and understanding of the requirements from contracting to the full lifecycle of the outsourcing deal. Competences and knowledge are required from outsourcing contracting, outsourcing compliance, (cloud) technologies, due diligence, auditing, risk assessment and service steering and monitoring. EBA recommendation considers whether the outsourcing institution maintains the skills and resources necessary to adequately monitor the outsourced activities (EBA 2017a, 13), or if the organization's staff has acquired the right skills and knowledge to perform effective and relevant audits and/or assessments of cloud solutions (ibid., 15). Further CEBS outsourcing guideline expects an organization to retain adequate core competence at a senior operational level in house to have the capability to resume direct control over an outsourced activity (CEBS 2006, 3).

11.1 Processing of data outside EU jurisdiction and power of European banking supervisory

According to EBA, institutions should take special care when entering into and managing outsourcing agreements undertaken outside the EEA because of possible data protection risks and risks to effective supervision by the supervisory authority (EBA 2017a, 17). Risk could realize in case outsourcing is agreed to take place under jurisdiction, where effective supervision by the supervisory authority is blocked.

11.2 Failure to contractually assure full rights of access and audit for both institutions and competent authorities

Regardless of the fact that large cloud service providers are seen reluctant to co-operate with granting the type of audit and access rights demanded by the recommendation, European Banking Authority is unwilling to make exceptions in its requirement of assuring the contractual rights for both institutions and competent authorities. Based on summarization of all the 37 responses submitted to draft recommendation consultation process, the concerns of securing the sufficient audit and access rights are illustrated in Figure 10. A single response can contain none or multiple aspects of concerns and can equal a higher figure than 37 in total. The summarization is based on information collected in Appendix 3.

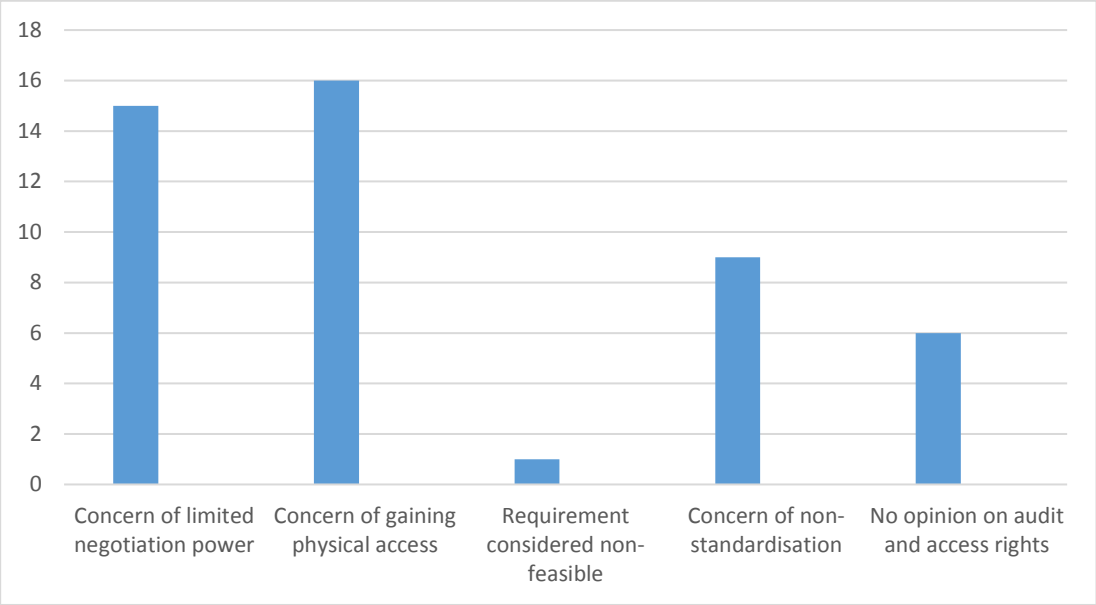

Figure 10: obstacles for getting full audit and access rights among EBA consultancy paper respondents

According to EBA (European Banking Authority 2017a, 47-48), in addition to physical access to the business premises of the cloud service provider, right of access also refers to the full range of devices, systems, networks and data used to provide the outsourced services. Further, the recommendation explicitly states there should be no contractual limitations to the outsourcing institution's right to audit or any form of fixed hierarchy in the way the rights are exercised to maintain flexibility (ibid., 49). Virtual or logical access is deemed to be de facto included in the audit tools both for institutions and competent authorities (ibid., 47).

In practice, this means financial organizations and financial service providers relying on any subcontractor or 3rd party platform or infrastructure provider must carefully consider if the contractual chain conforms to European Banking Authority's recommendations. As a case example, Microsoft (2017) Azure enables large financial institutions to enter into a separate contract amendment with Microsoft to meet their privacy, security and regulatory requirements as an entity subject to oversight by a regulator. By further analyzing Microsoft Guidance on complying with regulatory guidelines applicable to financial services institutions using Microsoft Azure in Singapore, the document suggests Microsoft (2016, 11) has a positive stance on

granting access and audit rights on a regulatory basis by stating “Another reason for the selection of Microsoft in this case is that it permits regulator audit and inspection of its data centers and in agreed circumstances inspection rights for its financial services customers”. Some of the audit and access support functions can be subject to fee-based yearly subscription such as Microsoft Online Services FSI Customer Compliance Program (Microsoft 2017, 1). Similar contract amendments and programs can exist for other cloud service providers and the point is that these are typically not included in the standard agreement or online service terms and covers only a limited service portfolio. Commercially, this type of special arrangements may involve significant cost elements, which mean the benefits of cloud would derive elsewhere than from plain hardware capacity pricing.

11.3 Failure to pass on contractual obligations to subcontractors or sub-processors

The outsourcing institution should agree to chain outsourcing only if the subcontractor will also fully comply with the obligations set between the outsourcing institution and the outsourcing service provider (European Banking Authority 2017a, 17). Although the cloud service provider is responsible for providing the service agreed with the outsourcing institution, the outsourcing institution should have oversight of the overall service provided regardless of whether it is provided through subcontractors (ibid., 66) even if there is no requirement to establish service monitoring spanning to subcontractor level.

11.4 Inadequate or ad-hoc SLA monitoring process

Outsourcing institution is obliged to review and monitor the performance of the overall service on an ongoing basis, regardless of whether it is provided by the cloud service provider or its subcontractors and evaluate against performance criteria set in the outsourcing contract (European Banking Authority 2017a, 16). Neglecting SLA monitoring and outsourcing management might lead to decrease of the standards of the outsourced service; the quality of the service is not as good as defined in service

contract or has missed opportunities to detect deteriorating service level before a major incident.

11.5 Inadequate or ad-hoc risk management process

Changes in e.g. cloud service supply chain is one example of events, which might affect the ability of the service provider to meet its responsibilities under the outsourcing agreement, and should trigger carrying out of a risk assessment by a financial institution. Extending the adoption of cloud services beyond the current scope through change management process could be another type of event, which could require a risk assessment to take place before approval.

11.6 Inadequate or ad-hoc change management practices and violation of cloud outsourcing policy

Over time, the outsourcing organization might change the way, how cloud services under a cloud service provider are consumed or the scope of adopted services expanded. In the worst case, the business risks are evaluated based on the original scope rather than against the updated range of services. Use of services, which do not comply with the compliance requirements, e.g. enjoy the same level of audit and access rights, demanded from the outsourcing financial institution, could raise a security incident due to non-compliance.

11.7 Operationalizing data subject rights

International Association of Privacy Professionals, a not-for-profit organization, together with TrustArc conducted a survey in September and October 2017 to subscribers of IAPP Daily Dashboard. The survey identified operationalizing the right to be forgotten and operationalizing data portability as top risks followed by obtaining and managing user consent, complying with international data transfer requirements and preparing for data breach notification (IAPP 2017, 3).

Providing an electronic copy of personal data to conform to data portability is a topic online banking channels need to address to. This is more of a problem on supporting

services capable of integrating information sources together holding customer master data and providing that preferably over a single API towards the online channels whereas online channels could format the data to human readable and presentable form.

Right to be forgotten in financial services context is a more complex process requiring closing of financial products such as accounts and loans before it is possible to terminate customer relationship and personal data from operative systems. However, by design online banking channels should not store personal data, but instead, rely on master information sources. In case of an exception, online banking channels could expose an API, which can be invoked to exit any personal data, rather than the opposite where a request would be made from the online banking channel to initiate the process.

Data processing regulation, security and subject rights must also be taken care of in outsourcing to cloud covering also the cloud service provider including cloud infrastructure provider. Additionally, the geographical location of processing must be considered.

11.8 Incapability to demonstrate compliance

According to EU GDPR Article 24, the controller shall implement appropriate technical and organizational measures to ensure and to be able to demonstrate that processing is performed in accordance with the regulation (European Parliament and the Council of the European Union 2016, 47). This means capability to document, where and how the data is processed or stored, and what are the technical and organizational controls to protect the data. In case there is no evidence backing up the defined controls and processes, that are documented, or the selected controls are not sufficient in comparison to the type of data processed, there is a risk of noncompliance and sanctions.

11.9 Processing data beyond the purpose of received consent

Processing of personal data is lawful only if the data subject has given explicit consent for one or more specific purposes; or it is necessary for the performance of a

contract to which the data subject is party; or in order to take steps at the request of the data subject prior to entering into a contract; or processing is necessary for compliance with a legal obligation, to which the controller is subject to. (European Parliament and the Council of the European Union 2016, 36). Financial institutions must be careful, e.g. what kind of targeted marketing or segmentation they can do based on financial and transaction data available of customers, what information they can directly request from the customer, or what data could be shared between business service partners without prompting for request of a consent.

11.10 Personal data breach notification and loss of reputation

In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the supervisory authority about the breach (European Parliament and the Council of the European Union 2016, 52). The notification must contain information where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned (ibid., 52). When the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall communicate the personal data breach to the data subjects (ibid., 52). In addition to being capable of collecting and analyzing forensics information within 72 hours in relation to the data breach, a financial institution would have to cope with the sanctions and reputational risks due loss of customer confidence and trust followed by a breach.

11.11 Vendor lock-in in cloud outsourcing

Whether the lock-in factor comes from e.g. data, technology, service or application lock-in, financial institutions should according to outsourcing guidelines avoid situations, where they cannot exit or recover from decreased performance of service provider. Vendor lock-in is a synonym for substitutability barrier or tells about neglected assessment of substitutability and exit planning (EBA 2017a, 18). Vendor lock-in could also occur in case the outsourcing institution no longer possesses enough understanding of the business processes or service being outsourced.

11.12 Unproven or missing disaster recovery capabilities

Considering how important self-service channels are for financial institutions, there should also be plans for cloud-based services, how to recover from failures on e.g. availability zone or a provider of DNS services. To effectively demonstrate that disaster recovery capabilities of cloud platform or service are used in the correct way, proper testing should be done. Testing is done to ensure there is no need for time-consuming and more radical architectural changes once the service is already published for live or during very late phase of delivery cycle. The same goes with backups to avoid an unacceptable level of data loss.

12 Discussion

12.1 Cloud outsourcing in general

The regulative landscape of outsourcing to cloud is permissive, however, there are requirements such as audit and access for the institution and competent authorities subject to the whole outsourcing chain, which are challenging to meet contractually. This was indicated by all the respondents of EBA consultancy paper as can be seen in Appendix 3. Standard contract agreements seldom comply, unless a cloud service provider is specifically targeting at serve financial institutions and/or there is high demand explicitly from financial service companies for the offering, making it commercially feasible for a cloud service provider to address compliance concerns specific for financial services industry.

There is little incentive to implement as few controls as possible by a financial institution; however, instead by centralizing common architectural building blocks and personal data repositories the most of the synergies can be exploited. By segregating the solution architecture to clearly defined components according to business domains, helps setting scope and boundaries for different auditing schemes and regulations. The same fundamental design thinking and aim of optimizing the synergies by having common building blocks could be applied to outsourced services in multi-vendor landscape assuming the suppliers are working in cloud-based custom

development domain or provide stateless utility services rather than focus on large volume market and standardized features.

12.2 Feasibility of cloud outsourcing

Outsourcing to cloud recommendation's provisions for material outsourcing, which require special attention during outsourcing planning, due diligence, contracting, risk management, auditing and service level monitoring, which means the scope of outsourced production workload in cloud should be relatively significant to be commercially feasible and to have a basis for a profitable business.

Factors increasing profitability are including but not limited to improved time-to-market, speed of development, automation and development feedback loop, and quality or business advantage of the financial service. The lower the value chain is, the higher volumes should be moved to the cloud to be profitable. In practical terms, buying plain capacity (low in value chain) is most likely not profitable unless volumes are relatively high due to the need to subscribe to programs or additional professional services, which guarantee sufficient audit and access rights for a financial institution. There could also be additional, significant costs in case solution architecture requires transformation to be deployed to cloud.

There are Nordic examples of profitable financial sector businesses run on even hyper-scale cloud infrastructure such as Holvi, offering digital banking services for entrepreneurs, and Solinor Payment Highway, which is an offering for accepting card payments online, both based on Amazon Virtual Private Cloud (Amazon VPC).

There is also an example of hybrid cloud architecture, where S-Bank offers marketing information about services on Microsoft Azure whereas they keep sensitive financial data outside public cloud (Microsoft 2015b, 2).

12.3 Key challenging cloud outsourcing requirements

The new Recommendations on Cloud Outsourcing by European Banking Authority are nothing revolutionary but rather conservative in the light of physical audit and access rights, which must be secured contractually covering also potential

subcontracting. The requirement can be seen as a principal one shared by both traditional outsourcing and cloud outsourcing models in financial sector. This might be an obstacle with certain types of cloud service providers and service delivery models even if at practical level a financial institution can choose to rely in risk-based manner to a trusted 3rd party or pooled audit results. The recommendation for financial institutions is also to regularly assess the content of the certifications or audit reports on an ongoing basis, and in particular, ensure that key controls are still covered in the scope of services adopted now and in the future.

Another challenging requirement on cloud outsourcing, where applicable, is having proper contingency plans and exit strategies in place for all cloud outsourcing arrangements. Considering outsourcing scope, complexity, potential use of proprietary technologies or IPRs, and speed of new innovations, securing the exit with full scope of services and without undue disruption to its provision of services or adverse effects on its compliance will continue to be a challenge.

12.4 Cloud outsourcing risk landscape

There are different layers in outsourcing risk landscape:

- macroprudential risks, which are monitored by supervising authorities based on the notifications of outsourcing deals done by financial institutions,
- risks depending on the complexity and scale of outsourcing in scope of a financial institution as a whole,
- and risks related to a specific outsourcing arrangement and performance of a supplier.

As described earlier in the thesis, the risk landscape from a financial institution's point of view, enriched with a couple of public case examples in Sweden, is well known and covered by EBA ICT risk assessment guideline. The guideline also covers:

- inadequate resilience of third party or another group entity services,
- inadequate outsourcing governance,
- as well as inadequate security of third party or another group entity.

In addition, fulfilling the compliance requirements could be highlighted as a forth item including, however, not limited to outsourcing arising from e.g. EU GPDR.

The importance of mitigating these risks derives from the threats including criminals who know that third party suppliers can be a weak link and target them accordingly.

12.5 Characteristics of compliance solution architecture

By comparing industry best practices for security and service architecture in online banking domain and the compliance requirements set by supervising authorities, it can be concluded that the level of compliance requirement setting is on very high-level with more focus on contracting, risk management and outsourcing management processes. There are also regulations and provisions for data protection and data subject rights, however, apart from encryption and data lifecycle management and a few functional level requirements related to the transparency and privacy settings, there is plenty of room for interpretation in translating them into the language of engineering and usability.

To ensure the compliance of solution and its architecture, it is proposed that its documentation covers traceability back to the requirements including a link or the original text of provision of regulation, guideline or recommendation, the interpretations, the implementation design, and how the solution relates to business and admin processes where it is intended to be used.

Outsourcing contract is a critical component of an outsourced compliance solution or service architecture including exact service description of the scope and context of outsourcing, assets, description of responsibilities between parties, KPIs, purpose of data processing and any items which are excluded or not considered to be part of the service e.g. non-transferrable intellectual property rights.

A technical security architecture and the security controls implemented by the solution, are not sufficient alone without being backed up by processes, which enable risk-based transparency in service management. The service contract must stretch to secure long-term business continuity of a financial institution and support handover of responsibilities as part of exit scenarios, whether it is terminated naturally by the expiry of the contract or triggered by deteriorated service levels.

Certification, not only in the area of information security management system but in a wider context, can be seen as a fast-track for a service provider to attract and acquire new customers and avoid security auditing effort overhead.

12.6 Adoption of ISMS for cloud outsourcing

One of the benefits of mapping compliance and regulative requirements to an information management system such as ISO-IEC 27001:2013 was the visibility gained: what type of controls and processes are required, where can synergies be found from existing controls, and what would be administrative burden and cost be expected to be associated with the compliance effort. Due to the fact that these types of requirements are on a high-level; standards, guidelines on how to apply the standards and industry best practices can help in finding approaches to actual implementations.

ISO-IEC 27001:2013 also seeks for commitment from top to down and by that ensures better chances to succeed in implementing a range of security controls and objectives according to plan of controls mapped against compliance requirements. Having clear reporting lines and KPIs helps to gain continuous support in information security management.

12.7 Inconsistencies of regulations and guidelines

By looking at different regulations and guidelines, it is apparent that there are plenty of conflicts between them both in area of outsourcing, especially subcontracting, and data protection. Because the renewed regulation and guidelines are just about to enter into force, it comes as no surprise, that there is a great deal of confusion about how to comply and what the best practices are.

Inconsistencies were reported by European Association of Co-operative Banks (2017, 19) in their reply to consultation on Fintech between PSD2 Access to Accounts (XS2A) and Portability of Data according to the EU GDPR Art. 20. Account servicing payment service providers under PSD2 are required to provide authorized PISPs and AISPs an access to customer account information subject to customer consent. This information includes sharing personal data. However, an ASPSP has no contractual relationship with PISP or AISP or has any means to ensure subject data protection rights of the 3rd party other than trusting the registry of PSD2 entities being supervised.

According to Working Party (2017b, 8), requests must be assessed on a case by case basis, how, if at all, such specific legislation, such as PSD2, may affect the right to data portability in general as meant in EU GDPR. Understanding how to interpret a regulatory requirement might require understanding of the hierarchy of different laws and their priorities to ensure correct practices in conflict of interests.

12.8 Reliability of the results

Many of the used information sources participated in commenting outsourcing to a cloud consultation paper and are practitioners in financial sector by role, or represented e.g. a legal firm rather than research studies or academic publications or relied on direct information from the authorities themselves. This means the research portrays more the practical concerns, issues and best practices that the type of organizations face in everyday life while implementing compliance requirements into working practices or controls. For the outsourcing part, the number of respondents to EBA's consultancy paper used as a basis for analysis was relatively large compared to the option that this type of interview was done privately to a selected group of respondents.

Considering the maturity of the subject matter, there was plenty of new information published all the time during the thesis research. For the quality of the research, it would have been beneficial to wait for more concrete case examples. The same applies to the interest that many Nordic financial institutions have just recently started to show on outsourcing based on As a Service delivery model.

12.9 Applicability of the thesis for other industries

The compliance architecture could be applied to any medium or large business according to the criteria for defining the size of a business by European Commission, and involving processing of personal data of EU citizens. Retail industry and e-commerce portals are good examples of sharing many of the security concerns due to processing of both personal data and online transactions. However retail industry is neither subject to same level of supervision and auditing by authorities nor

compliance reporting giving them more flexibility in adoption of cloud based solutions.

Considering the number of generic security requirements for the compliance architecture and effort required to monitor the outsourcing risks and performance, the architecture is not considered feasible for micro or small-sized business.

12.10 Areas of further development

Due to the fact that the outsourcing recommendation and EU GDPR are not yet effective at the time of writing, there is plenty of room for research focusing on decisions or sanctions and the justification of those based on security controls the personal data controller or processor have had in place.

Another area of further research could be a practical case study to test the exit scenario of a solution architecture in financial services domain and e.g. outlining a self-channel architecture, which is capable of recovering in multi-cloud environment.

References

Aarnio, A. 1999. Encyclopaedia iuridica Fennica VII: suomalainen oikeus-tietosanakirja. Helsinki: Suomalainen lakimiesyhdistys

Baker McKenzie. 2017. The EBA's draft Recommendations for Cloud Outsourcing. Article. Accessed 8 October 2017. Retrieved from http://www.bakermckenzie.com/-/media/files/insight/publications/2017/06/al_emea_ebasdraftcloudoutsourcing_june2017.pdf?la=en

Bucur, A. 2011. Banking 2.0: Developing a Reference Architecture for Financial Services in the Cloud. Accessed 30 September 2017. Retrieved from https://d1rkab7tlqy5f1.cloudfront.net/TBM/Over%20faculteit/Afdelingen/Engineering%20Systems%20and%20Services/People/Professors%20emeriti/Jan%20van%20den%20Berg/MasterPhdThesis/Ana_Bucur__Thesis_Final.pdf

Chastanet, P. 2017. Codes of Conduct. Accessed 26 November 2017. Retrieved from http://ec.europa.eu/newsroom/document.cfm?doc_id=42973

Cloud Security Alliance, 2012. SecaaS Implementation Guidance - Category 8: Encryption. Accessed 28 October 2017. Retrieved from https://downloads.cloudsecurityalliance.org/initiatives/secaas/SecaaS_Cat_8_Encryption_Implementation_Guidance.pdf

Cloud Security Alliance, 2017. CSA response to European Banking Agency consultation paper on outsourcing to cloud service providers. Accessed 28 October 2017. Retrieved from https://www.eba.europa.eu/regulation-and-policy/internal-governance/recommendations-on-outsourcing-to-cloud-service-providers?p_p_auth=KgdQzc8k&p_p_id=169&p_p_lifecycle=0&p_p_state=maximized&p_p_col_id=column-2&p_p_col_pos=1&p_p_col_count=2&_169_struts_action=%2Fdynamic_data_list_display%2Fview_record&_169_recordId=1927111&_169_redirect=https%3A%2F%2Fwww.eba.europa.eu%2Fregulation-and-policy%2Finternal-governance%2Frecommendations-on-outsourcing-to-cloud-service-providers%2F-%2Fregulatory-activity%2Fconsultation-paper

Committee of European Banking Supervisors. 2006. Guidelines on outsourcing. Accessed 28 October 2017. Retrieved from https://www.eba.europa.eu/documents/10180/104404/GL02OutsourcingGuidelines.pdf.pdf

Danske Bank. 2018. Description of Danske Bank A/S, Finland Branch's customer register. Accessed 16 March 2018. Retrieved from https://www.danskebank.fi/PDF/en/Verkkopalvelut/Danske_Bank_Plc_Description_of_file.pdf

Data Protection Working Party. 2014. Opinion 05/2014 on Anonymisation Techniques. Accessed 8 December 2017. Retrieved from http://www.dataprotection.ro/servlet/ViewDocument?id=1085

Data Protection Working Party. 2017a. Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high

risk" for the purposes of Regulation 2016/679. Accessed 2 December 2017. Retrieved from ec.europa.eu/newsroom/document.cfm?doc_id=44137

Data Protection Working Party. 2017b. Guidelines on the right to data portability. Accessed 2 December 2017. Retrieved from https://ec.europa.eu/newsroom/document.cfm?doc_id=44099

Dutch Banking Association (Nederlandse Vereniging van Banken), 2017. Response to Consultation paper: Draft recommendations on outsourcing to cloud service providers. Accessed 28 October 2017. Retrieved from https://www.eba.europa.eu/regulation-and-policy/internal-governance/recommendations-on-outsourcing-to-cloud-service-providers?p_p_auth=8mVnKxTq&p_p_id=169&p_p_lifecycle=0&p_p_state=maximized&p_p_col_id=column-2&p_p_col_pos=1&p_p_col_count=2&_169_struts_action=%2Fdynamic_data_list_display%2Fview_record&_169_recordId=1915600&_169_redirect=https%3A%2F%2Fwww.eba.europa.eu%2Fregulation-and-policy%2Finternal-governance%2Frecommendations-on-outsourcing-to-cloud-service-providers%2F-%2Fregulatory-activity%2Fconsultation-paper%2F1848356

Elix-IRR Partners. 2011. Trends in Outsourcing & Offshoring in the Financial Services Industry 2008-2011. Accessed 23 February 2018. Retrived from https://www.elixirr.com/wp-content/uploads/2015/08/elix-irr-research_trends-in-fs-oo_nov2011_full_v2.pdf

Ernst & Young LLP. 2015. ISO 19600 International standard for compliance management. Accessed 22 February 2018. Retrived from http://www.ey.com/Publication/vwLUAssets/EY-iso-19600-international-standard-for-compliance-management/$FILE/EY-iso-19600-international-standard-for-compliance-management.pdf

European Association of Co-operative Banks. 2017. The EACB response to the European Commission consultation on fintech: A more competitive and innovative European financial sector. Accessed 1 December 2017. Retrived from https://v3.globalcube.net/clients/eacb/content/medias/publications/position_papers/digitalisation_and_the_use_of_data/final_eacb_response__ec_fintech_consultation.pdf

European Banking Authority. 2017a. Recommendations on outsourcing to cloud service providers. Accessed 16 September 2017. Retrived from https://www.eba.europa.eu/regulation-and-policy/internal-governance/recommendations-on-outsourcing-to-cloud-service-providers

European Banking Authority. 2017b. Guidelines on ICT Risk Assessment under the Supervisory Review and Evaluation process (SREP). Accessed 28 October 2017. Retrived from https://www.eba.europa.eu/documents/10180/935249/EBA-GL-2014-13+(Guidelines+on+SREP+methodologies+and+processes).pdf

European Banking Federation. 2017. Competitiveness of European Banks and Financial Technology. Accessed 16 September 2017. Retrived from http://www.ebf.eu/facts_and_figures/competitiveness-of-european-banks/

European Commission. 2014. A comprehensive EU response to the financial crisis: substantial progress towards a strong financial framework for Europe and a banking union for the Eurozone. Accessed 16 September 2017. Retrived from http://europa.eu/rapid/press-release_MEMO-14-57_en.htm

European Commission. 2018. PbD : Privacy by Design. Accessed 16 March 2018. Retrived from https://ec.europa.eu/eip/ageing/standards/ict-and-communication/data/pbd-privacy-design_en

European Council. Model Contracts for the transfer of personal data to third countries. Accessed 26 November 2017. Retrived from http://ec.europa.eu/justice/data-protection/international-transfers/transfer/index_en.htm

European Parliament and the Council of the European Union. 2016. Regulation (EU) 2016/679 of the European Parliament and of the Council. Article 87. Accessed 19 November 2017. Retrived from http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN

European Payments Council. 2010. The use of audit trails in security systems: guidelines for European banks. Accessed 14 January 2018. Retrived from https://www.europeanpaymentscouncil.eu/sites/default/files/KB/files/EPC153-10-Audit-Trails-in-Security-Systems-v1.0-Approved.pdf

European Union Agency for Network and Information Security (ENISA). Cloud Computing Information Assurance Framework. Accessed 1 October 2017. Retrived from https://www.enisa.europa.eu/publications/cloud-computing-information-assurance-framework/at_download/fullReport

European Union Agency for Network and Information Security (ENISA). 2015. Secure Use of Cloud Computing in the Finance Sector. Accessed 31 October 2016. Retrived from https://www.enisa.europa.eu/publications/cloud-in-finance/at_download/fullReport

Federal Deposit Insurance Corporation. 2014. Tools to Manage Technology Providers' Performance Risk: Service Level Agreements. Accessed 21 January 2018. Retrived from https://www.fdic.gov/news/news/financial/2014/tools-to-manage-technology-providers.pdf

Financial Times. 2017. Sweden grapples with huge leak of confidential information. Accessed 28 October 2017. Retrived from https://www.ft.com/content/d9e15fe4-7051-11e7-aca6-c6bd07df1a3c?mhq5j=e6

Finansinspektionen. 2016a. Tillsynen över bankerna och kreditmarknadsföretagen. Report. Accessed 1 October 2017. Retrived from http://www.fi.se/contentassets/480963a01b0745ae93f9267a0244a0ef/banktillsyn2016.pdf

Finansinspektionen. 2016b. Decision FI Ref 15-9258. Accessed 16 September 2017. Retrived from http://www.fi.se/contentassets/50b21dfc22d549d8a7b421a3f37718f9/nasdaq-clearing-2016-12-12-eng.pdf

Finansinspektionen. 2017a. Finansinspektionen's response to the Commission Consultation Document on FinTech: a more competitive and innovative European Financial Sector. Accessed 16 September 2017. Retrived from http://www.fi.se/contentassets/6ff715b42b0342cf99ae9046930f3617/eu-svar_fintech_bilaga.pdf

Finansinspektionen. 2017b. Myndighetens roll kring innovationer. Accessed 23 February 2018. Retrived from http://www.fi.se/contentassets/d3cd30fe473d4a7995f0c38209ddb7f1/myndighetens-roll-kring-innovationer.pdf

Finansinspektionen. 2018. Finansinspektionens syn på revisionsrätten för verksamhet som läggs ut på molntjänstleverantörer. Accessed 25 March 2018. Retrived from https://www.fi.se/contentassets/dba14943af5442c4b248730f915e0e30/fis-syn-molntjanster-20180312.pdf

Finanssialan Keskusliitto. 2009. Guidelines on bank secrecy. Accessed 26 November 2017. Retrived from http://www.finanssiala.fi/en/material/Guidelines_on_bank_secrecy.pdf#search=banking%20secrecy

Finanssivalvonta. 2013. Operatiiviset riskit valvojan näkökulmasta. Accessed 23 February 2018. Retrived from http://www.actuary.fi/uutiset/tapahtumat/oletko-sina-yhtiosi-operatiivinen-riski-operatiiviset-riskit-vakuutusalalla-19.11.2013/Koponen.pdf

Finanssivalvonta. 2015. Toimintakertomus 2015. Accessed 23 Febryary 2018. Retrived from http://www.finanssivalvonta.fi/fi/Tiedotteet/Toimintakertomukset/Documents/Finanssivalvonnan_toimintakertomus_2015.pdf

Finanssivalvonta. 2017a. Public consultation on FinTech: a more competitive and innovative European financial sector. Accessed 16 September 2017. Retrived from http://www.finanssivalvonta.fi/fi/Saantely/Lausunnot/Documents/Fivan_vastaukset_komission_FinTech-konsultaatioon.pdf

Finanssivalvonta 2017b. Supervisory Disclosure. Accessed 28 March 2018. Retrived from http://www.finanssivalvonta.fi/en/Supervision/Supervisory_Disclosure/Pages/Default.aspx

Gartner. 2018. IT Glossary: Business Process Outsourcing (BPO). Accessed 24 February 2018. Retrived from https://www.gartner.com/it-glossary/business-process-outsourcing-bpo/

Haller J. and Wallen C. 2016. Managing third party risk in financial services organizations: a resilience-based approach. Accessed 26 February 2018. Retrived from https://resources.sei.cmu.edu/asset_files/WhitePaper/2016_019_001_473742.pdf

Hall, M. 2011. Coding Case Law for Public Health Law Evaluation. A Methods Monograph for the Public Health Law Research Program (PHLR). Accessed 26 February 2018. Retrived from

http://publichealthlawresearch.org/sites/default/files/downloads/resource/CodingCaseLaw-Monograph-Hall2011.pdf

Holsti, O. 1969. Content Analysis for the Social Sciences and Humanities. Reading: Addison-Wesley.

IAPP. 2017. Getting to GDPR Compliance: Risk Evaluation and Strategies for Mitigation. Accessed 22 January 2018. Retrieved from https://iapp.org/media/pdf/resource_center/GDPR-Risks-and-Strategies-FINAL.pdf

IBM. 2017. IBM response to European Banking Authority Consultation Paper. Accessed 8 December 2017. Retrieved from https://www.eba.europa.eu/regulation-and-policy/internal-governance/recommendations-on-outsourcing-to-cloud-service-providers?p_p_auth=FAeBU0kq&p_p_id=169&p_p_lifecycle=0&p_p_state=maximized&p_p_col_id=column-2&p_p_col_pos=1&p_p_col_count=2&_169_struts_action=%2Fdynamic_data_list_display%2Fview_record&_169_recordId=1926566&_169_redirect=https%3A%2F%2Fwww.eba.europa.eu%2Fregulation-and-policy%2Finternal-governance%2Frecommendations-on-outsourcing-to-cloud-service-providers%2F-%2Fregulatory-activity%2Fconsultation-paper%2F1848356

ISO. 2014. ISO/IEC 27018:2014 Information technology -- Security techniques -- Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors. Accessed 25 February 2018. Retrieved from https://www.iso.org/standard/61498.html

ISO/IEC 19600:2014. Compliance management systems — Guidelines. Accessed 1 October 2017. Retrieved from https://www.iso.org/obp/ui/#iso:std:iso:19600:ed-1:v1:en

ISO/IEC29100:2011. Information technology — Security techniques — Privacy framework. Accessed 1 October 2017. Retrieved from https://www.iso.org/obp/ui/#iso:std:iso:19600:ed-1:v1:en

Kaplan, D & Powell J & Woller, T. 2016. AMD memory encryption. Accessed 21 January 2018. Retrieved from http://amd-dev.wpengine.netdna-cdn.com/wordpress/media/2013/12/AMD_Memory_Encryption_Whitepaper_v7-Public.pdf

Krippendorff, K. 2013. Content Analysis an Introduction to Its Methodology. 3 p. Thousand Oaks: SAGE Publications.

Leavy, P. 2014. Fundamentals of Qualitative Research. New York: Oxford University Press.

Lundberg E, Åkersson C. 2015. Cloud Computing - Factors that affect an adoption of cloud computing in traditional Swedish banks. Uppsala University. Master's Thesis.

Microsoft. 2015a. Announcing expanded Microsoft Azure support for financial services customers. Accessed 1 January 2018. Retrieved from https://azure.microsoft.com/en-us/blog/announcing-expanded-microsoft-azure-support-for-financial-services-customers/

Microsoft. 2015b. Finnish Bank Sharpens Competitive Edge with Online Banking Powered by a Hybrid Cloud Platform. Accessed 14 January 2018. Retrieved from https://info.microsoft.com/rs/157-GQE-382/images/WE-FI-S-Bank-Case%20Study-Microsoft.pdf

Microsoft. 2016. Microsoft guidance on complying with regulatory guidelines applicable to financial services institutions using Microsoft Azure: Singapore. Accessed 1 January 2018. Retrieved from http://download.microsoft.com/download/C/D/D/CDDA963E-B5A8-4FDD-9CFE-3412186ECC95/Singapore_FSI_Checklist_Azure_4_October_2016_FINAL.pdf

Microsoft. 2017. Microsoft Cloud Agreement Financial Services Amendment. Accessed 1 January 2018. Retrieved from http://www.nevcom.co.uk/wp-content/uploads/2017/06/MCA_FSIAm_WW_ENG_May2017.pdf

Nordea. The processing of personal data in Mobile Bank app. Accessed 16 March 2018. Retrieved from https://www.nordea.fi/en/personal/our-services/online-mobile-services/processing-of-personal-data-in-mobile-bank.html

OWASP. 2017. Transport Layer Protection Cheat Sheet. Accessed 21 January 2018. Retrieved from https://www.owasp.org/index.php/Transport_Layer_Protection_Cheat_Sheet#Rule_-_Use_TLS_or_Other_Strong_Transport_Everywhere

PricewaterhouseCoopers AG. 2017. The EU General Data Protection Regulation (GDPR) in the banking industry An impact analysis on banks and wealth managers with the focus on Switzerland. Accessed 8 December 2017. Retrieved from https://www.pwc.ch/en/publications/2017/gdpr_banking_industry_report_en.pdf

Reuters. 2017. Swedish PM calls potential IT leak 'disaster' and risk to country. Accessed 28 October 2017. Retrieved from http://www.reuters.com/article/us-sweden-securityleak/swedish-pm-calls-potential-it-leak-disaster-and-risk-to-country-idUSKBN1A926F?il=0

Saarenpää, A. 1998. Oikeusinformatiikka. Accessed 16 September 2017. Retrieved from http://lipas.uwasa.fi/materiaalit/talousoikeus/it/oikeusinformatiikka12005.pdf

Segovia, A. 2015. The ISO 27001 & ISO 22301 Blog. Accessed 18 November 2017. Retrieved from https://advisera.com/27001academy/blog/2015/08/25/iso-27001-vs-iso-27032-cybersecurity-standard/

Seipel, P. 2010. IT Law in the Framework of Legal Informatics. Accessed 16 September 2017. Retrieved from http://www.scandinavianlaw.se/pdf/47-2.pdf

Svantesson, D. 2012. Data protection in cloud computing – The Swedish perspective, Computer Law & Security Review Volume 28, Issue 4.

Temenos. 2017. Response to Consultation paper: Draft recommendations on outsourcing to cloud service providers under Article 16 of Regulation (EU) No 1093/2010. Accessed 28 October 2017. Retrieved from https://www.eba.europa.eu/documents/ddm/com.liferay.portlet.dynamicdatalists.model.DDLRecord/1924883/ddm-fileupload15941

Whitman, E & Woszczynski A. 2004. The Handbook of Informatoin Systems Research. 309 p. London: Idea Group Publishing.

Yle. 2015. Verkkopankki horjuu mutta kaatuu harvoin – katkoja vahditaan valppaasti. Article. Accessed 14 October 2017. Retrieved from https://yle.fi/uutiset/3-8214697

Yle. 2016. Nordea myöntää: Verkkopankin takkuilu ei ole hyväksyttävää. Article. Accessed 14 October 2017. Retrieved from https://yle.fi/uutiset/3-8660458.

Appendices

Appendix 1. Mapping of EBA recommendations on outsourcing to cloud against ISO-IEC 27001 and ENISA Information Assurance Framework control objectives and controls

ISO 27001:2013 & ENISA IAF control	EBA recommendation on outsourcing to cloud	Number of requirements
Information security policies (ISO 27001 - A.5)	CEBS Guideline (only) 6: outsourcing institution should have a policy on its approach to outsourcing, including contingency plans and exit strategies	1
Organization of information security (ISO 27001 - A.6)	CEBS Guideline (only) 2: responsibility for the proper management of the risks lies with an outsourcing institution's senior management. Responsibility cannot be outsourced.	1
Human resource security (ISO 27001 - A.7) Personnel security (ENISA IAF - 66.1)		0
Asset management (ISO 27001 - A.8) Asset management (ENISA IAF - 6.5)	16 a. Identify and classify its activities, processes and related data and systems as to the sensitivity and required protections	1
Access control (ISO 27001 - A.9) Identity and access management (ENISA IAF - 6.4)	16 a. Identify and classify its activities, processes and related data and systems as to the sensitivity and required protections	1
Cryptography (ISO 27001 - A.10) Key management (ENISA IAF - 6.4.4) Encryption (ENISA IAF - 6.4.5)	16 c. Institutions should also consider specific measures where necessary such as the usage of encryption technologies in combination with appropriate key management architecture for data in transit, data in memory, and data at rest.	1
Physical and environmental security (ISO 27001 - A.11) Physical security (ENISA IAF - 6.8), Environmental controls (ENISA IAF - 6.9)	16 a. Identify and classify its activities, processes and related data and systems as to the sensitivity and required protections	1
Operations security (ISO 27001 - A.12) Operational security (ENISA IAF - 6.3)	16 a. Identify and classify its activities, processes and related data and systems as to the sensitivity and required protections	1

Communications security (ISO 27001 - A.13) Network architecture controls (ENISA IAF - 6.3.3)	16 a. Identify and classify its activities, processes and related data and systems as to the sensitivity and required protections 16 c. Institutions should also consider specific measures where necessary such as the usage of encryption technologies in combination with appropriate key management architecture for data in transit, data in memory, and data at rest.	2
System acquisition, development and maintenance (ISO 27001 - A.14)	16 a. Identify and classify its activities, processes and related data and systems as to the sensitivity and required protections 16 c. Institutions should also consider specific measures where necessary such as the usage of encryption technologies in combination with appropriate key management architecture for data in transit, data in memory, and data at rest.	2
Supplier relationships (ISO 27001 - A.15) Supply chain assurance (ENISA IAF - 6.2)	6. Written agreement with CSP including right to audit, right to access 7. Contractual agreements should not impede exercise of right of access or audit 8. Exercising the right to audit in risk based manner 14. Prior notification of a planned visit and cooperation of supplier written in agreement 15. Guideline 8 (2) (b) and 9, outsourcing institutions with respect to quality and performance should feed into written contract and SLAs. 17. Contractual obligation to protect data confidentiality, continuity of activities outsourced, integrity and traceability of data and systems also in accordance with specific measures (controls) identified as necessary 18. Monitor the performance of activities and security measures in line with CEBS guideline 7 including incidents, on an ongoing basis and review as appropriate. Take any corrective measures thereto. 21; 22; 24. Agreeing of use and rules of subcontracting and setting forth compliance obligations in contract.	11

	27 c. Obligation in agreement to CSP to orderly transfer the activity and that of the subcontractors to another SP or to the direct management of the outsourcing institution in case of exit clause 23. Risk assessment of impacts in case of changes in subcontracting 25. The outsourcing institution should review and monitor the performance of the overall service on an ongoing basis regardless whether it is provided by CSP or its subcontractors	
Information security incident management (ISO 27001 - A.16) Incident management and response (ENISA IAF - 6.7.1)	The recommendations do not include specific requirements for reporting of security incidents by institutions to their competent authorities in the context of cloud outsourcing (p. 24)	0
Information security aspects of business continuity management (ISO 27001 - A.17) Business continuity management (ENISA IAF - 6.7)	9. Maintaining relevant register of information on material and non-material outsourcing activities 15; 26; 27 a; 28 a, c. Guideline 6 (6) (e) institutions should implement arrangements to ensure the continuity of the services provided by the outsourcing service provider. Policy should include contingency planning and a clearly defined exit strategy 27 b; 28 d. Transition plan and validation in terms of testing for the case of transferring existing outsourcing activities. Define success criteria for the plan. 28 a; 29. The outsourcing institution should include indicators that can trigger the exit plan in their ongoing service monitoring and oversight of the services provided by their CSP	4
Compliance (ISO 27001 - A.18)	1; 16 b. Materiality assessment (compliance documentation) 2. Duty to adequately inform supervisors and provide and maintain relevant register of information on outsourcing (compliance reporting and documentation) 3. Risk analysis for the material activities outsourced (compliance documentation) 4; 5. Maintain relevant register of information on material and non-material outsourcing activities (compliance documentation)	6

	9. Acquiring of right skills and knowledge to perform effective and relevant audit and/or assessment of cloud solutions (knowledge and skills) 19; 20. Take special care when entering into and managing outsourcing agreements undertaken outside the EEA due to possible data protection risks and risks to effective supervision	
Legal requirements (ENISA IAF - 6.10)	20	1
Data and services portability (ENISA IAF - 6.6)	Indirectly same as 15; 26; 27 a; 28 a, c. Guideline 6 (6) (e)	0

Appendix 2. Mapping of EU GDPR requirements for processor against ISO-IEC 27001 and ENISA Information Assurance Framework control objectives and controls

ISO 27001:2013 & ENISA IAF control	**EU GDPR Article summary**	**Number of requirements**
ISO 27001 - Chapter 3	Article 4: Definitions Definitions should be aligned with any information security classifications an organization may have impacting selected security controls for processing	1
ISO 27001 - A.9.4.2 Secure log-on procedures ENISA IAF - 6.4.5: Encryption ENISA IAF - 6.4.7: Credential compromise or theft	Article 87: Processing of the national identification number Member States may further determine the specific conditions for the processing of a national identification number or any other identifier of general application. Swedish Data Protection Authority: *Dataskyddsutredningen som har föreslagit att sådana uppgifter ska få behandlas bara om det är klart motiverat med hänsyn till ändamålet med behandlingen, vikten av en säker identifiering eller något annat beaktansvärt skäl. Bestämmelsen motsvarar tidigare bestämmelse i personuppgiftslagen. (*Datainspektionen. 2017).	1
ISO 27001 - A.5 - A.18	1. f) Personal data is processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures ('integrity and confidentiality') Article 32 The controller and the processor shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate: 2. the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services	By approaching this requirement in terms of ISO 27001 this would mean 114 controls to be in place.
ISO 27001 - A.17.1.2 Implementing information security continuity	Article 32 The controller and the processor shall implement appropriate technical and organizational measures	2

ISO 27001 - A.17.1.3 Verify, review and evaluate information security continuity	to ensure a level of security appropriate to the risk, including inter alia as appropriate: 3. the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident 4. a process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing	
ISO 27001 - A.18.1.1 Identification of applicable legislation and contractual requirements	Article 1: Subject-matter and objectives Article 2: Material scope of processing Article 3: Territorial scope Article 28 Processor incl. assists the controller in ensuring compliance with the obligations pursuant to Articles 32 to 36 taking into account the nature of processing and the information available to the processor Article 31 Cooperation with the supervisory authority Article 32 Security of processing Artcicle 33 The processor shall notify the controller without undue delay after becoming aware of a personal data breach Article 34 Communication of a personal data breach to the data subject Article 35 Data protection impact assessment Article 36 Prior consultation	6 plus requirements referred from Article 28
ISO 27001 - A.18.1.4 Privacy and protection of personally identifiable information	Article 32 The controller and the processor shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk	6
ISO 27001 - A.10.1.1 Policy on the use of cryptographic controls	Article 32 The controller and the processor shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:	2

ISO 27001 - A.18.1.5 Regulation of cryptographic controls ENISA IAF - 6.4.5: Encryption	1. which may include pseudonymisation or encryption of personal data	

Appendix 3. Obstacles for getting full audit and access rights among EBA consultancy paper respondents

Organization	Response to audit and access right	Interpretation of practicality
Association of Financial Markets in Europe (AFME)	AFME views that the requirements for securing rights to access and audit could be an obstacle for financial institutions when outsourcing to Cloud Service Providers (CSPs)	Problematic contractually
Alternative Investment Management Association (AIMA)	Access to business premises: Requiring physical access to where data is stored may make it impossible for asset management firms to use public cloud services. We therefore consider that datacenters should be specifically carved out of the references to "business premises" and "operations centers" in paragraphs 6(a), 10(a), 14(a) and 14(b) or the right of physical access to datacenters should be substituted for a right of access to the relevant systems information. In other words, seeing racks of blinking lights is of little use but being able to see infrastructure diagrams and setup might be useful. Increasingly physical infrastructure is being replaced with Software-defined Infrastructure so there is nothing to actually see – or it could be split over multiple locations on shared physical infrastructure;	Problematic due physical access
Asociación Española de Banca (AEB)	Two main challenges arise when negotiating contract arrangements with CSPs: (i) CSPs reluctance or inability to assume contract terms in practice (e.g. user's and supervisor's right to audit), and (ii) CSP are not always willing neither to negotiate their template contracts to accommodate to different regulations and national or entity specificities nor to include non-regulated issues into contractual arrangements	Problematic contractually
Association of Foreign Banks (AFB)	The FCA guidelines1 acknowledge that a visit from a regulator may be disruptive to the provider as well as having security implications.	Problematic due physical access
Banking & Payments Federation Ireland (BPFI)	While institutions pursue access and audit rights for all cloud outsourcing, institutions may not always secure this right with all CSPs due to practical implications on providers around allowing access to physical datacenters and the security implications. It is therefore suggested that institutions in such cases may rely on third party certification and third party audit reports.	Problematic due physical access
Financial Conduct Authority	The FCA guidelines1 acknowledge that a visit from a regulator may be disruptive to the provider as well as having security implications. Conversely, the EBA guidelines require further clarification as to potential disruption and security issues	Problematic due physical access
Cloud Infrastructure Services Providers in Europe	We welcome the draft recommendation in paragraph 7 that an outsourcing institution and cloud provider should agree upon "alternative ways" to provide assurance "when the performance of audits or the use of certain audit techniques might create a risk for another client's environment." This seems to imply, but	Problematic due physical access

	does not explicitly state, that the EBA recognizes physical access to premises, such as data centers, presents risks to cloud infrastructure and customer data that should be avoided. To promote convergence on how financial institutions exercise their access and audit rights, it would be welcomed if the EBA would clearly define what is meant with using “alternative ways” to achieve assurance.	
Cloud Security Alliance	Are there any specific recommendations regarding access to datacenters? Guidance from other bodies such as the FCA recognizes/accepts datacenters may be treated differently by CSPs when considering access to business premises e.g. “…for legitimate security reasons, may limit access to such sites – such as data centers. And …does not necessarily include data centers.” Is an abridged extract from the FCA finalized guidance FC16-5 document. CSA STAR is widely acknowledged as the leading security assurance programme for Cloud Security. STAR encompasses key principles of transparency, rigorous auditing, and harmonization of standards. Furthermore, tools like CSA STARWatch can help organizations manage/streamline compliance efforts.	N/A
Czech Banking Association (CBA)	One of the EBA recommendations on outsourcing to cloud providers is "unrestricted rights of inspection and auditing" which is according to our experience difficult to enforce to the contracts with cloud providers. Further clarifications should be provided and therefore, we would appreciate to have specific examples of conditions which are considered as acceptable.	Problematic contractually
DXC TECHNOLOGY	Access and audit rights are of paramount importance to any OSP (Cloud provider) due to security and contractual requirements. Complete access to data and external rights of inspection and audit cannot be granted due to the nature of the services provided and confidentiality requirements. Furthermore the audit access should only apply to service locations and not all business locations. Access by a third party and full access by a statutory auditor including devices, systems etc may fall foul of contractual requirements of clients this therefore may not be acceptable in public or virtual private where services are delivered in a multi-tenant environment. Customer’s auditors shall have no access to any shared infrastructure or to data concerning other DXC customers or DXC operations.	Problematic contractually and due physical access
Deutsche Bank AG	Applying the ‘traditional’ access and audit rights concept to cloud outsourcing services is a major obstacle in practice, as cloud providers strongly push back on the inclusion of the full range of access and audit provisions. This reflects the fact that CSPs are	Problematic contractually and due physical access and non-

	providing highly standardized services to a large volume of customers. This business model is not comparable to traditional outsourcing relationships, which are much more bespoke. At its core, public cloud provides is a commodity service – it is consistent no matter the client and thus designed accordingly. The right to on-site audits is not an accepted industry standard for CSPs and its introduction leads to prolonged contract negotiations. It is typically a red-line for most CSPs due to issues of confidentiality and privacy of other customer's data, and interference of the standard processes on which cloud services are provided. Further, physical access is also less beneficial given the increasing dispersion of data across facilities and even countries.	standard approach
Deutsche Börse Group	Particularly the prescribed right to physical access to relevant business premises of the cloud service provider should be further clarified in order to avoid unnecessary requests to physical access to e.g. datacenters, systems and networks of cloud service providers, which might result in a disproportionate burden for cloud service providers and thereby create itself an operational risk. Burdensome regulations on excessive audit rights might hinder potential cloud service providers to offer services to the financial industry and as such might lead to insufficient and concentrated offers of cloud solutions.	Problematic contractually and due physical access
Division Bank and Insurance Austrian Federal Economic Chamber	Should the compliance with this framework not exclusively be placed on banks, which do not have the ability to impose their conditions to CSPs	Problematic contractually
Dutch Banking Association (Nederlandse Vereniging van Banken)	NVB considers full right of access for institutions at major cloud service providers quite unrealistic. Individual financial institutions lack the bargaining power to receive this right to access. NVB concludes that most European banks likely won't be able to exercise this right of access. This is not the case in the US and consequently this results in an unlevel playing field with US based banks.	Problematic contractually
ESBG	EBA should consider including in section 4.3 dispositions ensuring that virtual access to data, with continuous monitoring capabilities for the outsourcing institution, is granted to outsourcing institutions and competent authorities. Otherwise, these recommendations risk of soon becoming irrelevant in practical terms. Two main challenges arise when negotiating contract arrangements with CSPs: (i) CSPs are not always able to comply with specific contract terms in practice (e.g. user' and supervisor's right to audit), and (ii) CSP are not always willing neither to negotiate their template	Problematic contractually and physical access

	contracts in order to accommodate to different regulations and national or entity specificities nor to include non-regulated issues into contractual arrangements. The position CSPs are adopting in contractual negotiations arise from the fact that they are not required to comply with the regulatory and supervisory rules banks are entitled to.	
Electronic Money Association	The recommendations that the outsourcing institution ensures that the CSP outsourcing agreement provides "to the institution's statutory auditor full access to the CSP business premises" in Section 4.3 (Clause 6a) and "unrestricted rights of inspection and auditing (right of audit)" (Clause 6b) ignore the dynamics of the business relationship between financial service providers and the larger, global CSPs. The latter serve tens of thousands of outsourcing entities using hundreds of locations. It is unlikely that an outsourcing institution could secure access to all CSP business premises; instead, we propose that the focus of access is on CSP premises and processes directly involved in the delivery of the services of the outsourcing institution.	Problematic contractually and non-standard approach
Eurofinas	We appreciate the coherent approach adopted by the EBA on the basis of risk and proportionality. The guidelines' clarification on the ability for an outsourcing institution to fulfil its audit obligations through pooled audits and third-party certifications is especially important for small and medium-sized institutions. The possibility of pooled audits together with other clients of the same cloud service provider allows for the more efficient usage of relevant and highly specialized expertise with the minimum level of disruption and risk for other cloud clients' environment and data. In this context, we believe that further guidance would be beneficial to further clarify the necessary qualifications of competent third-party auditors and certifiers.	N/A
EUROPEAN ASSOCIATION OF CO-OPERATIVE BANKS	Access and auditing rights are usually the most challenging part of the negotiation with cloud service providers. These requirements are not included in standard contract terms and need usually additional contractual provision. Cloud service providers usually prefer third party auditing which they can publish to all clients instead of separate audits made by every single client. The possibility to use third party certifications and pooled audit with other clients are therefore warmly welcomed.	Problematic contractually and non-standard approach
European Banking Federation	Physical access to premises hosting the cloud infrastructure is often a point of tension in negotiations with CSPs, who may be reluctant to allow customers into their datacenters for legitimate security and confidentiality reasons. Furthermore, in a globalized and distributed cloud model, access to the physical location delivers a negligible outcome, other than the most basic one of physical security and access checks.	Problematic contractually and due physical access

Finance Denmark	The requirements in section 6 (a) and (b) implies that the outsourcing company and its auditor should, as a rule, have full access to the supplier's right of access and unrestricted rights of inspection and audit. These requirements are very far-reaching and, moreover widespread than what is applicable after the outsourcing guidelines. It can be assumed that the requirements will be difficult to get a supplier to accept and, incidentally, customer initiated, customer-specific physical inspection / audit is not the most appropriate method of securing deliveries either from a cost or security point of view.	Problematic contractually and due physical access
Finance Norway	-	N/A
German Banking Industry Committee	Securing the right to access and audit (paragraphs 6 to 14) is a major obstacle for financial institutions in outsourcing to CSPs. Requiring every institution to have access to the CSP is not feasible and may actually increase the overall security risk to the CSP (i.e. more people on premises). An alternative solution, which still addresses the risk / concerns of these outsourcing arrangements, would be to allow financial institutions to leverage existing industry standards and certifications of CSPs, which cover many requirements proposed by the EBA. As pointed out in chapter 3 (Background and rationale – fourth paragraph, last sentence), large Cloud Service Providers (CSPs) may be seen to constitute critical infrastructure for (the financial) industry – in a similar fashion to major internet service providers. Hence, institutions cannot be made to bear the burden of auditing CSPs of this caliber.	Problematic due non-feasibility and physical access
HyTrust	-	N/A
IBM	IBM recommends the EBA consider this approach as an alternative to individual FI physical examination and audit of compliance of CSP Data Centers IBM is concerned that an unrestricted approach to the introduction of financial industry wide physical audit access rights to Cloud Service Provider (CSP) Data Centers, will increase operational risk to the Financial Services Sector, not diminish it, and that this is counter intuitive to the aims of using a secure cloud outsourced solution. IBM strongly believes there is need to focus on cloud relevant audit and control improvement opportunities, and to avoid reliance on traditional legacy systems audit and control approaches. To this end, IBM strongly recommends the regulatory recognition, or adoption, of independent third party audits based on recognized international standards e.g. American Institute of Certified Public Accountants (AICPA) Trust Services Principles or equivalent	Problematic due physical access and non-standard approach

	International Standard for Assurance Engagements (ISAE3402)	
Interessengemeinschaft Kreditkarten	IK suggests to explicitly consider the concept of multi-tenant service providers with respect to access and audit rights in DR 4.3 in a proportionate manner and to build on it as a frequently applied standard in the IT-processing industry by addressing specific practical requirements of multi-tenant service providers. In this context it is proportionate as EBA suggested to either apply pooled customer audits or that institutions be provided by the cloud provider with external audit reports considering compliance with industry IT-security standards and certification requirements such as compliance with ISO 27000 standards and auditing and reporting on data protection compliance.	Problematic due non-standard approach
London Stock Exchange Group	We observe that it is often difficult to get cloud providers to disclose their regulatory compliant terms, and ultimately, is often a matter of negotiation with cloud providers. Although these arrangements are often seen as outsourcing by regulators, the cloud terms do not always match up to the standards required of outsourcing documentation. As a cloud user, we note that guidance provided by the EBA and various other regulators is helpful, but if providers do not adhere to it, then it restricts our ability to use them and to fully leverage from the benefits of cloud. We believe that it would be beneficial for regulators to provide further clarity and take a more flexible/risk based approach to the definition of what constitutes "cloud outsourcing", as treating all cloud services as "outsourcing" inhibits a regulated customer taking up the benefits that cloud provides considering cloud suppliers are often reluctant to adhere to traditional outsourcing terms in contracts.	Problematic contractually
Microsoft	We recommend that the EBA further emphasize the risks which physical audits of datacenters can create and the need to take an appropriate and proportionate approach in this regard. Protecting the confidentiality, integrity and security of data and overall systems is of the utmost importance to financial institutions and their customers. Physical audits of datacenters, as opposed to other cloud provider business premises, upon which services are provided to hundreds or thousands of financial institutions creates unnecessary risk where the same level or higher levels of oversight can be achieved by alternative means. As most regulators recognize, actual on-site audits of datacenters is unnecessary and obtaining information and underlying evidence of controls and their implementation, is what matters from a supervisory perspective. Thus, it is the mechanisms under which cloud providers make such information available that is important. So long as customers who have a need to	Problematic due physical access

	obtain information can obtain access to it, including through self-help tools offered at scale, this should be sufficient to meet audit requirements without imposing undue burdens on either cloud providers or financial institutions.	
Nasdaq	In the context of access and audit rights (section 4.3), Nasdaq believes that it would be more appropriate to require outsourcing agreements to include a right for competent authorities to access "relevant business centers" of the cloud outsourcing provider, rather than "head offices", as this may not be relevant for the particular services provided under the relevant arrangement. Also, very extensive audit and access rights, that also include areas not immediately relevant to the particular service, may not be possible to achieve in relation to the service providers.	Problematic due unlimited access and audit rights
PayPal Europ	We welcome the possibility for the outsourcing institution to use a range of tools in addition to its own audit resources: third-party certification, third party audits and pool audits.	N/A
Pinsent Masons	Auditing the provision of an IT service is a very different scenario from the many other scenarios in which financial institutions must meet auditing requirements in respect of how their businesses are conducted. The EBA should focus on the principle of proportionality in making recommendations regarding the extent to which auditors and regulators require access to information and premises in order to conduct audits of cloud services and acknowledge that rules which are necessary in other auditing contexts are not appropriate and need not to be followed in a technology service provision context. As a key example, the value of physically inspecting datacenters in terms of assessing the risk of the services being provided is widely acknowledged as being extremely low.	Problematic due physical access
Swift	SWIFT understands the EBA is proposing that outsourcing institutions ensure they have agreements with cloud service providers in place and in writing. Further the EBA proposes that such agreements should stipulate that the cloud service providers undertake the obligation to allow access to its business premises and gives unrestricted rights to inspection and auditing by the outsourcing institutions. While we understand the EBA's overarching intent with this proposal, we believe that these measures are redundant where alternative existing arrangements are already in place, which serve the same purpose and meet the same objectives as the recommendations set out in this proposal.	Problematic due non-standard approach

Smart Payment Association	-	N/A
Standard Chartered	In general, with regards to audit provision and its intended purpose with respect to CSPs, one of the reasons CSPs do not permit access to datacenters is because of their security requirements, and given the nature of this industry there often may not be much information to gain from direct access to a physical center. As such, it might be more helpful to the outsourcing institution if CSPs demonstrate that their processes were properly performing their roles, for example in systems operations centers, instead of focusing on the specifics of negotiating contractual terms, notice periods and fees. This may be more beneficial and result in a better outcome in terms of security. For instance, CSPs could be required to have their own audits, covering specific issues identified by and agreed across regulators, which would then be disclosed to all their clients and regulators.	Problematic due physical access and non-standard approach
Temenos	In the case of a public cloud utilizing a virtualized environment, a visit to a datacenter will not practically assist in obtaining access to data or devices and will be of limited benefit. Large datacenters are extremely secure and the locations of the centers are confidential. Visitors to a datacenter create a security risk and hyper scale datacenter providers do not encourage such visits. Most cloud providers would expect the institutions and its auditors to rely on formal certifications from third parties.	Problematic due physical access and non-standard approach
Verband der Auslandsbanken in Deutschland e.V. | Association of Foreign Banks in Germany	Regarding the provision set out in lit. a), it has to be taken into account that it will be unrealistic for all users of cloud services and their auditors to have "full access" to the business premises of the cloud service providers. Not only do cloud service providers have multiple business premises around the world and data from one institution or group might be stored in multiple jurisdictions due to cost efficiency and capacity of the cloud service provider, but also due to security reasons a diversification on different premises is often made. Keeping the "on premises control tourism" out of all facilities is part of the security plan of most cloud service providers. Both location of such premises and the exact handling of data storage is part of the service providers' business secret. Therefore, it is foreseeable that it is hardly impossible for relatively small customers of cloud service providers to negotiate access to business premises as well as insight into the security infrastructures of cloud service providers into the outsourcing contract. Such scenario might be possible for those customers representing a high value to the service provider but certainly not for all customers.	Problematic contractually and due physical access

Yorkshire Building Society Group	-	N/A
BBVA	These recommendations should include the possibility of replacing the access and audit right in case the CSPs hold Third Party certifications recognized by Competent Authorities. Certification processes would mitigate a side effect that will become relevant as CSPs have a higher number of Financial Institutions as customers. Indeed, it would be very difficult to assist auditors appointed by each of their customers, as this continuous affluence of auditors could disrupt their activities. Moreover, given the nature of cloud services, having access to the data center where data are located is an unattainable requirement, since data are usually distributed and replicated among different data centers. Given that introducing these requirements in contracts with CSPs, whose services are not only offered to Financial Institutions, is usually burdensome for Financial Institutions, the creation of a mechanism that guarantees that CSPs are aware of the requirements above and accept them, would ease the negotiation with CSPs and foster cloud adoption.	Problematic contractually, due non-standard approach and physical access